

FortiPortal Administration and User Guide

Version 5.0.0

FORTINET DOCUMENT LIBRARY

<http://docs.fortinet.com>

FORTINET VIDEO GUIDE

<http://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTIGATE COOKBOOK

<http://cookbook.fortinet.com>

FORTINET TRAINING SERVICES

<http://www.fortinet.com/training>

FORTIGUARD CENTER

<http://www.fortiguard.com>

END USER LICENSE AGREEMENT

<http://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdocs@fortinet.com



August 1, 2018

FortiPortal Administration and User Guide

TABLE OF CONTENTS

Change log	9
Part I: Administration Guide	10
FortiPortal overview	11
Key features	11
Special characters	11
Components	11
End-customer devices	13
FortiPortal concepts	13
FortiPortal installation	15
VMware prerequisites	15
Downloading OVF files	16
Installing FortiPortal VMs	16
Start the VM or vApp	18
Basic setup	18
Sizing	18
Default login credentials	19
Database installation	19
Portal installation	20
Collector installation	23
FortiManager configuration	25
FortiAnalyzer configuration	26
Additional setup tasks	27
Reset your password	28
Change Password	29
Alerts	30
Page actions	30
Administrative users	31
Page actions	31
Per-user actions	31
Create a user	31
Trusted Hosts	33
Admin user roles	34
Dashboard	35

Initial data-aggregation delay.....	36
Setting the top N entries.....	36
Customers.....	37
Page actions.....	37
Per-customer information.....	37
Per-customer actions.....	38
Add or edit a customer.....	39
Customer sites.....	45
Page actions.....	45
Per-site actions.....	45
Wireless Networks.....	47
Page actions.....	47
Per-network actions.....	47
Customer Users.....	49
Page actions.....	49
Per-user actions.....	49
Add or edit a customer user.....	50
Add a trusted host for a user.....	51
Customer user roles.....	52
Reports.....	54
FortiPortal reports.....	54
Page actions.....	54
Per-report actions.....	54
FortiAnalyzer reports.....	55
Page actions.....	55
Per-report actions.....	56
FortiManager devices.....	57
Page actions.....	57
Per-FortiManager actions.....	57
FortiManager high availability (HA).....	58
Add a FortiManager.....	59
Edit a FortiManager.....	59
Manage FortiGate devices.....	60
AP controller devices.....	62
Page actions.....	62
Per-controller actions.....	62
Edit a controller.....	63
FortiAnalyzer devices.....	65
Prerequisites.....	65
Page actions.....	65
Per-FortiAnalyzer actions.....	65

Edit a FortiAnalyzer.....	66
View FortiAnalyzer reports.....	67
FortiPortal collectors.....	68
Page actions.....	68
Collector high availability (HA).....	68
Add a FortiPortal collector.....	69
Per-collector actions.....	70
Edit a collector.....	70
Admin settings.....	72
Remote authentication using FortiAuthenticator.....	74
RADIUS server configuration.....	76
RADIUS Roles.....	77
Remote authentication—SSO.....	80
Frequently asked questions (FAQs) about SSO configuration.....	82
SNMP.....	84
SNMP agent.....	84
SNMP v1/v2c communities.....	86
SNMP v3 users.....	89
SNMP MIBs.....	91
SNMP traps.....	91
Fortinet and FortiPortal MIB fields.....	93
Roles.....	94
Page actions.....	94
Per-role actions.....	94
System Log.....	96
Page actions.....	96
Initial log-aggregation delay.....	96
Theme.....	97
Custom theme options.....	97
Select a predefined color scheme.....	97
Create a custom color scheme.....	97
Using the color picker.....	98
Using a custom CSS file.....	101
Custom URLs and text.....	101
Custom images.....	103
Resizing images.....	104
Details of the theme configuration fields.....	104
System Info.....	107
License Information.....	107
Upload a license.....	108
Version Information.....	108

FPC Admin Login.....	108
Certificate Information.....	109
Trusted Hosts.....	110
Page actions.....	110
Per-role actions.....	110
Additional Resources.....	112
Page actions.....	112
Per-role actions.....	113
Audit.....	114
Page actions.....	114
Per-audit actions.....	114
Upgrading FortiPortal software.....	116
Upgrade procedures.....	117
Alert messages.....	120
Service-provider level messages:.....	120
Customer-level messages:.....	121
Appendix: Sizing.....	122
Appendix: Installation using OpenStack.....	127
Prerequisites.....	127
Downloading FortiPortal image files.....	127
OpenStack Horizon Dashboard.....	127
Create images for the portal and collectors.....	127
Create volumes for the portal and collector.....	128
Launch the instances.....	128
Assign a floating IP address.....	129
Associate the volume to the instances.....	129
Reboot the instances.....	129
Determine the IP address and port number.....	129
Configure the portal parameters.....	130
Configure the collector parameters.....	131
Updating the SSL certificate file.....	132
Installing MySQL for FortiPortal databases.....	133
Reconfiguring MySQL password on FortiPortal.....	133
Part II: User Guide.....	135
FortiPortal web interface.....	136
Landing page.....	137
Reset password.....	138
Change Password.....	139
Alerts.....	140
Page actions.....	140
Dashboard.....	141

Page actions.....	142
Widget actions.....	142
View	144
Application view.....	144
Attack view.....	145
Sandbox view.....	146
Wireless Networks	147
Reports	148
FortiPortal reports.....	148
Report definition actions.....	148
Run Now actions.....	149
Per-report actions.....	149
FortiAnalyzer reports.....	150
Rogue AP	151
Additional Resources	152
Policy	153
Policy tab column settings.....	153
Policy data refresh.....	153
Revision backup.....	153
Creating and restoring policy revisions.....	154
Configuring policies.....	154
Adding a new policy.....	154
Updating a policy.....	154
Deleting a policy.....	154
Enabling or disabling a policy.....	155
Policy fields.....	155
Moving a policy.....	157
Re-installing the policy.....	158
Reviewing policies.....	158
Objects	159
Types of objects.....	159
Zone/Interface.....	159
Firewall Objects.....	160
Security Profiles.....	161
User & Device.....	162
Configuring objects.....	164
Adding a new object.....	164
Updating an object.....	164
Deleting an object.....	164
Audit	165
Page actions.....	165

Per-audit actions.....	166
Device Manager	167
VPNs	168
Configuring VPNs.....	168
Creating an IPSec phase-1 or phase-2 configuration.....	168
Updating an IPSec phase-1 or phase-2 configuration.....	168
Deleting an IPSec phase-1 or phase-2 configuration.....	168
IPSec phase-1 fields.....	169
IPSec phase-2 fields.....	171
Routes	173
Configuring static routes.....	173
Adding a new static route.....	173
Updating a static route.....	173
Deleting a static route.....	173
Static route fields.....	174

Change log

Date	Change Description
May 30, 2018	Initial release for FortiPortal 5.0.0
June 1, 2018	Fixed the title bar and updated the “FortiPortal installation” chapter.
July 11, 2018	Updated the “FortiPortal installation” chapter.
July 16, 2018	Added the “SNMP” chapter.
August 1, 2018	Updated the “Upload a license” section.

Part I: Administration Guide

FortiPortal overview

FortiPortal enables a Managed Security Service Provider (MSSP) to operate a cloud-based hosted security management and log retention service. The service provides the MSSP end-customers with centralized reporting, traffic analysis, configuration management, and log retention without the need for the end customer to invest in additional hardware and software.

Key features

FortiPortal provides the following features:

- dashboard widgets for system and log status
- log viewer with filters
- drill-down analysis of user and network activity
- report generator (with customization options)
- wireless network status
- device management
- policy management
- Remote authentication using FortiAuthenticator

FortiPortal supports the following languages: Romanian, French, Portuguese, Spanish and English.

Special characters

In releases prior to 2.40, you could include some special characters (quote and backslash) in controller names. For example, the following name would be valid:

```
Name ' 1 / 3
```

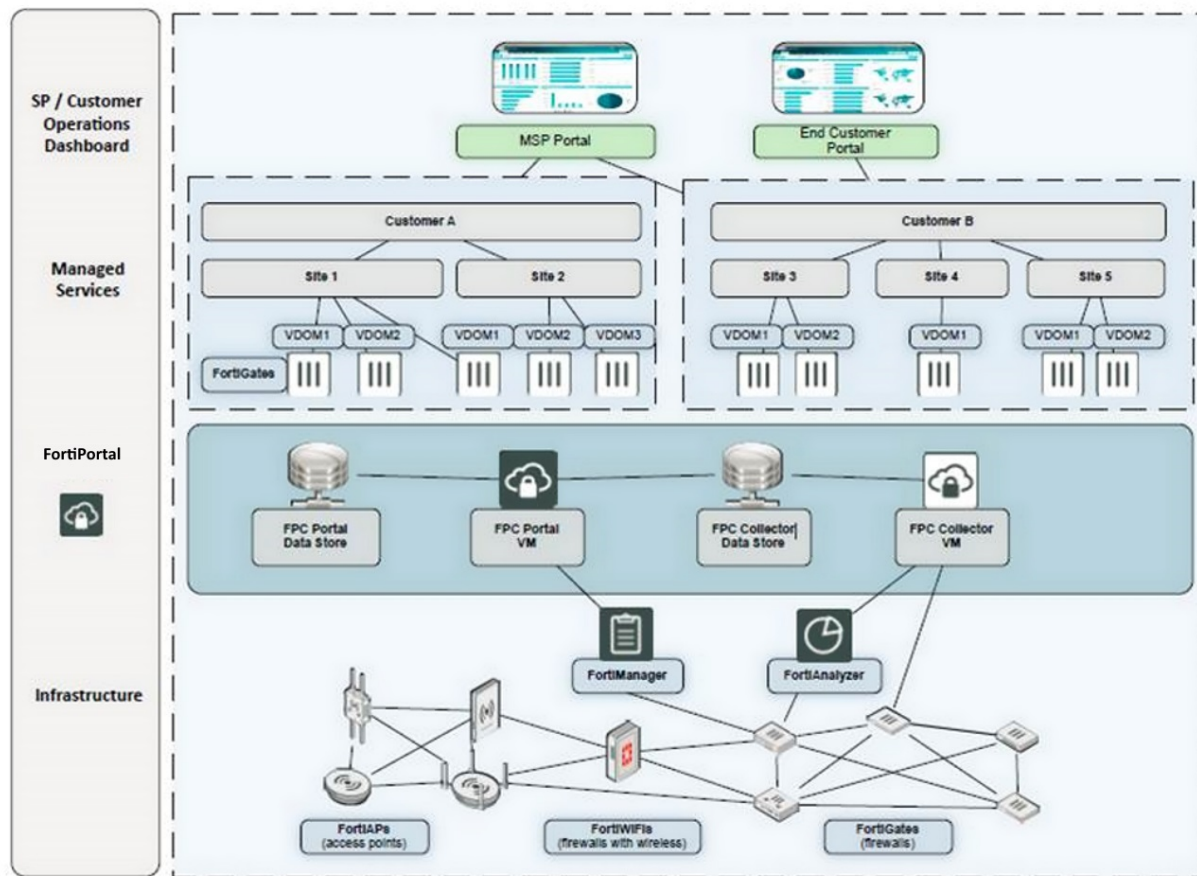
However, in release 2.4.0 and later, you must not use these characters. Prior to upgrading to release 2.4.0, you must remove these special characters from existing names.

Components

The end-customer's FortiGate devices are managed by one or more FortiManagers. Optionally, logs from the FortiGate devices can be gathered by one or more FortiAnalyzers.

In the FortiPortal, the collectors collect logs from the FortiAnalyzer (or the FortiGate devices directly) and store the logs in collector databases. The portal aggregates the logs into a central database, and performs security analytics on the logs. The portal provides an administrative web interface (for the service provider administrative staff) and a customer web interface (for the MSSP's customers).

The following figure illustrates the FortiPortal components and a typical customer network.



The FortiPortal solution includes the following components:

- Collector: virtual appliance:
 - Manages logs sent from the FortiGate devices
 - FortiPortal can include more than one collector
- Collector database: MySQL database:
 - Physical or virtual server provided by the service provider
 - The collector stores the logs in this database
 - FortiPortal can include more than one collector database
- Portal: virtual appliance:
 - Provides the service provider web interface and the customer web interface.
 - Uses the FortiManager API to manage devices, objects, and policies
 - FortiPortal includes only one portal (however, the portal can consist of multiple VM instances for redundancy and/or scalability)
- Portal database: MySQL database:
 - Physical or virtual server provided by the service provider
 - The portal aggregates the logs into this database
 - FortiPortal includes only one portal database

The customer web interface enables each end customer to access/analyze their data and administer their service. For additional information about the customer web interface, see the [FortiPortal User Help](#) (which is also available by selecting the help button in the customer web interface).

The administrative web service allows the service provider to configure the services for each end customer, and to manage the overall cloud service.

End-customer devices

FortiPortal requires that the customer FortiGate devices must be managed by FortiManager. FortiManagers may reside in the customer network or in the MSSP cloud.

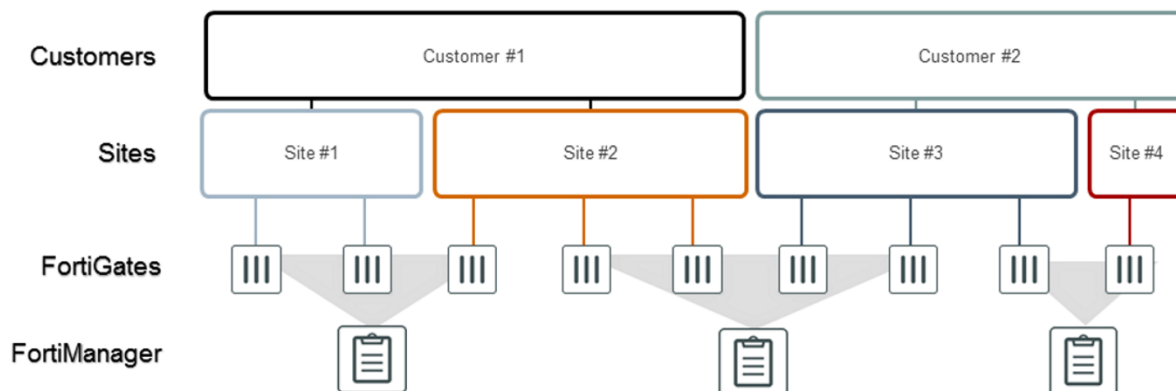
1. FortiGate: security devices in the customer environment:
 - generates the security logs
 - passes logs to the collector
 - also fulfills the AP Wireless Controller role
2. FortiManager: manages a set of FortiGate devices:
 - All FortiGate devices in the FortiPortal must be managed by FortiManager
 - FortiManager provides device information to the FortiPortal
 - May reside in the customer network or in the MSSP cloud
3. (Optional) FortiAnalyzer: receives logs from the devices:
 - passes the logs on to the collector
 - May reside in the customer network or in the MSSP cloud

FortiPortal concepts

FortiPortal introduces the following concepts:

Customer sites

- An end-customer can have multiple sites.
- A site is a logical grouping of devices (independent of which FortiManager manages the device).
- Devices are FortiGate devices or AP wireless devices.



Storage limits

- Each end-customer has a storage capacity maximum amount, which is expressed as a number of GB of database storage.
- The storage capacity is allocated between the two databases. The allocation is configurable per-customer. The default allocation is as follows:
 - Portal database (20% of the customer's storage amount)
 - Collector databases (80% of the customer's storage amount)

If a customer exceeds their storage limit, one of the following strategies is applied (this is configurable for each customer):

- Overwrite the oldest logs
- Stop logging

Remote authentication

You have the choice of local or remote user authentication of the Admin and Customer portal users. Local authentication works by defining the users in the local user databases. Remote authentication provides a choice of Radius authentication or FortiAuthenticator. The choice of authentication method is global to the whole FortiPortal.

If you set the authentication mode to remote, all user management functions reside with the remote system. FortiPortal user management capabilities (add/modify/delete users, reset password, change password) are blocked, as these apply only to local users.

For additional information regarding FortiAuthenticator, refer to the [FortiAuthenticator product documentation](#).

Trusted Hosts

If you are using local user authentication, you can add the Trusted Hosts capability as an added level of security. You can apply the Trusted Hosts capability as a global feature. Optionally, you can add per-customer whitelists.

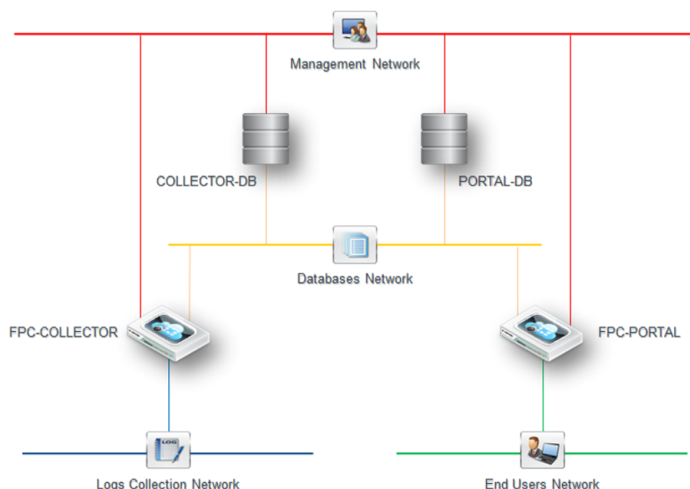
If you enable Trusted Hosts as a global setting, the system enforces a configurable blacklist and configurable whitelist for all admin and customer users.

You can also enable Trusted Hosts as a customer setting. The system creates a whitelist of trusted hosts for the customer users. The default entry in the whitelist is to allow all users, so you need to delete this entry to create a real whitelist.

NOTE: For a customer with Trusted Hosts enabled, the system also enforces the global blacklist and whitelist for the customer users.

FortiPortal installation

The following figure shows an example of a FortiPortal topology:



This chapter covers the following tasks:

- ["VMware prerequisites"](#) on page 15
- ["Basic setup"](#) on page 18
- ["Additional setup tasks"](#) on page 27

FortiPortal software provides a self-service management interface for managed security service provider (MSSP) customers (or any organization that uses FortiManager to manage security instances) to monitor and configure security instances without direct FortiManager access. FortiPortal is a web application and runs on virtual machines where each VM runs one of the following:

- Portal VM (which is the external interface for FortiManager)
- Portal database server VM
- Collector VM (which is used for analytics)
- Collector database server VM (MariaDB 10.2 and MySQL 5.7 are the recommended database servers.)

The basic installation requires four VMs. (Portal load balancing and collector high availability (HA) configurations, discussed later, add additional VMs.)

NOTE: Remember to protect FortiPortal with an external firewall. External users should only connect to the portal VM. They should not make direct connections to the database servers, collector VMs, or FortiManager.

VMware prerequisites

For KVM and OpenStack, see ["Appendix: Installation using OpenStack"](#) on page 127.

This chapter assumes some familiarity with the VMware vSphere Client terminology.

Before deploying your FortiPortal using VMware, you must do the following:

1. Install the VMware vSphere Client on the management computer.
2. All VM instances run on VMware ESXi Server version 5.5 or later.
3. You must install one database server for the portal database and one database server for each collector database instance.

FortiPortal provides two installation alternatives. The choice of alternative determines the required OVF files that you need to download.

- Install the portal and collector as individual VMs. Required files for a new VMware installation:
 - fpcvm64imageCollector.out.ovf.zip
 - ffpcvm64imagePortal.out.ovf.zip
- Alternatively, both VMs can be installed as a virtual app. Required file:
 - fpcvm64imagevApp.out.ovf.zip

Downloading OVF files

To download the required OVF files, follow these steps:

1. Navigate to the Fortinet customer service page (support.fortinet.com).
2. Go to *Download > Firmware Images*.
3. On the Firmware Images page, select *FortiPortal*.
4. Download the latest versions of the required zip files.
5. Extract the packages to a local folder on the management computer.

Installing FortiPortal VMs

You have a choice of VM installation methods. You can install separate VM instances for the portal and each of the collectors, or you can install the portal and collector as a VM vApp.

Installing the portal and collectors includes the following major steps:

1. Create a VM instance or a VM vApp. See "[Create a VM instance](#)" on page 16 or "[Create a VM vApp](#)" on page 17.
2. Configure VM hardware settings. See "[Configure VM hardware settings](#)" on page 18.
3. Power on the VM. See "[Start the VM or vApp](#)" on page 18.
4. Configure the portal or collector parameters.

The first time you start the portal, you will have access only through the console window of your VM server environment. After you configure the initial parameters, you can access the FortiPortal through the web-based portal.

Create a VM instance

NOTE: This VM is intended for testing purposes only and should not be used for production environments.

1. Download the portal or collector OVF file.
2. Launch the VMware vSphere client.
3. Enter the IP address or host name of your VMware server.

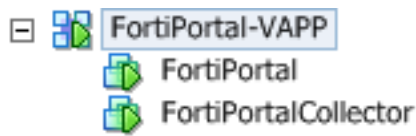
4. In the inventory menu, select the physical server where you will install the VM.
5. Select *File > Deploy OVF Template* to launch the OVF Template wizard. The wizard will guide you through a series of deployment steps.
6. *Source*: Use the Browse function to locate the OVF file:
 - Portal: FortiPortal-VM64.ovf
 - Collector: FortiPortal-VM64-Collector.ovf
7. *OVF Template Details*: This page displays the following information: FortiPortal version, size of the download, and application size on disk. Select *Next*.
8. *End-user License Agreement*: Accept the end-user license agreement and select *Next*.
9. *Name and Location*: Enter a name for this virtual machine, select a location from the location inventory and select *Next*.
10. *Storage*: Select the destination storage for the virtual machine files and select *Next*.
11. *Disk Format*: This page displays the storage device that you selected in the previous step, along with available space. Select *Thin Provision* and select *Next*.
12. *Network Mapping*: Select the destination network to map to the source network in your OVF and select *Next*.
13. *Ready to Complete*: Review the deployment settings. Select *Back* to make any changes. When ready, select *Finish*.

Create a VM vApp

NOTE: As a convenience, vApp contains the MySQL image for testing FortiPortal setups.

1. Download the application OVF file.
2. Launch the VMware vSphere client.
3. Enter the IP address or host name of your VMware server.
4. In the inventory menu, select the physical server where you will install the VM.
5. Select *File > Deploy OVF Template* to launch the OVF Template wizard. The wizard will guide you through a series of deployment steps.
6. *Source*: Use the Browse function to locate the OVF file for the application:
 - fpcvm64imagevApp.out.ovf.zip
 - or
 - fpcvm64imagevApp-mysql.out.ovf.zip
7. *OVF Template Details*: This page displays the following information: FortiPortal version, size of the download, and application size on disk. Select *Next*.
8. *End-user License Agreement*: Accept the end-user license agreement and select *Next*.
9. *Name and Location*: Enter a name for this VM vApp, select a location from the location inventory and select *Next*.
10. *Storage*: Select the destination storage for the virtual machine files and select *Next*.
11. *Disk Format*: This page displays the storage device that you selected in the previous step, along with available space. Select *Thin Provision* and select *Next*.
12. *Network Mapping*: Select the destination network to map to the source network in your OVF and select *Next*.
13. *Ready to Complete*: Review the deployment settings. Select *back* to make any changes. When ready, select *Finish*.

The system creates a VM vApp using the name that you provided in step 9, as shown in the following figure:



Configure VM hardware settings

If required, adjust the VM CPU, memory and storage settings. The following are the default settings:

- CPU: 2
- Memory: 2 GB
- Hard drive: 80 GB

To adjust these numbers, select the newly created VM in the inventory list and select *Getting started > Edit virtual machine settings*.

Start the VM or vApp

In the inventory list, right-click the FortiPortal VM or vApp that you just installed and select *Power On*.

Basic setup

NOTE: The portal interacts with FortiManager, and the collector, typically, interacts with FortiAnalyzer. To avoid the portal or collector becoming a bottleneck, you can adjust their maximum CPU and memory sizes so that they equal the values for the FortiManager and FortiAnalyzer devices they interact with.

Basic setup covers the following tasks:

- "Sizing" on page 18
- "Default login credentials" on page 19
- "Database installation" on page 19
- "Portal installation" on page 20
- "Collector installation" on page 23
- "FortiManager configuration" on page 25
- "FortiAnalyzer configuration" on page 26

Sizing

FortiPortal sizing can be complex. Fortinet recommends that you work with your Fortinet systems engineer when possible. However, using the following guidelines, you can successfully complete this task:

- Portal VM—The default storage disk size is 80 GB, which is the recommended minimum. (The 2-GB disk in the VM is the flash memory; the 80-GB disk is storage.) If you have many customer logins and many devices, then increase the memory and disk sizes for improved performance.
- Collector VM—The storage disk size depends on the number of FortiGate units logging to it. The default 80-GB storage supports approximately 20 FortiGate units. (You can increase the disk size to support more FortiGate units. But a single collector has a maximum rate of 15,000 logs per second.)

- Portal and collector databases server VMs—The minimum customer (database) storage size is 5 GB, which comfortably supports about 100 logs per second with an aggregate log retention period of 30 days. Of this 5 GB, by default, 80 percent is stored in the collector database as raw logs and 20 percent is stored in the portal database as aggregate logs. (You can adjust this value to increase storage for aggregate logs.) So, for an 80/20 split, 4 GB is required for the collector database and 1 GB for the portal database. For example, if you have 100 customers, you need a minimum 500-GB database storage with the default 5-GB storage: 100 GB for portal and 400 GB for collector. Configure the database servers to accommodate growth because these require the most storage. For example, start with 1 TB or more, each, for the portal and collector database servers. You then set the size of both the portal and collector databases in the FortiPortal application.

(See ["Appendix: Sizing"](#) on page 122 for further information about sizing. Using VMs, you can easily increase the amount of memory or disk sizes with Logical Volume Manager [LVM].)

Default login credentials

The following are the default user names and passwords for the FortiPortal components:

Component	Default User Name	Default password
Portal	admin	No password
Collector	admin	No password
Portal database VM	fpc	fpc
Collector database VM	fpc	fpc
Portal database and collector database (MySQL)	root	admin

Database installation

NOTE: Fortinet does not provide this server as part of FortiPortal. Fortinet supports the databases created by FortiPortal and the connections to them.

The following is the overall installation procedure, which starts by configuring the database servers:

1. After you create the database server image, you must install at least two instances, one for the portal database and one for each collector database.
2. Create the server VM and install the database server. FortiPortal supports MariaDB 10.2 and MySQL 5.7.
3. Install the portal. The portal requires a license.
4. Install the collector(s). (No licenses are required for the collector, so you can add as many collectors as needed if you need more log storage and an increased logging rate.)
5. After FortiPortal is running, you can add FortiManager devices and set up customers. See ["Add a FortiManager"](#) on page 59 and ["Add or edit a customer"](#) on page 39.

After you create the server VM and install the database server, configure the following settings in MySQL (version 5.7 or later) or MariaDB (version 10.2):

1. Set the MySQL server `bind-address` and `sql_mode` parameters in the `[mysqld]` section of one of the following files:

For MariaDB: `/etc/mysql/my.cnf`

For MySQL: `/etc/mysql/mysql.conf.d/mysqld.cnf`

For example:

```
[mysqld]
...
bind-address = 10.220.64.121
...
sql_mode = STRICT_TRANS_TABLES,NO_ZERO_IN_DATE,NO_ZERO_DATE,ERROR_FOR_DIVISION_
BY_ZERO,NO_AUTO_CREATE_USER,NO_ENGINE_SUBSTITUTION
```

2. From the MySQL console, use the `show variables` command to check that the following parameters are correctly set:

```
mysql -u root -p
```

3. Create a user for the portal, grant privileges to the user, and check that the user is created:

```
create user '<database_user_name>'@'%' identified by '<database_user_
password>';
GRANT ALL PRIVILEGES ON *.* TO '<database_user_name>'@'%' IDENTIFIED BY
<database_user_password>;
flush privileges;
```

```
# Use the following query to check that the user and host are entered correctly
select host,user from mysql.user;
```

For example:

```
> create user 'fpc'@'%' identified by 'fpc';
> GRANT ALL PRIVILEGES ON *.* TO 'fpc'@'%' IDENTIFIED BY 'fpc';
> flush privileges;
> select host,user from mysql.user;
```

Portal installation

NOTE: Before doing the portal installation, Fortinet recommends taking a snapshot of the portal database server in its initial state. If there are any errors installing portal, you can revert the database server to its initial state.

1. Install the portal VM image. For a new VMware installation, use the `fpcvm64imagePortal.out.ovf.zip` file. For the KVM version, see ["Appendix: Installation using OpenStack"](#) on page 127.
2. Configure the CLI settings. For example:

```

config system global
set hostname portal # use whatever name that you want to give the VM
set timezone 28 # use ? to identify the correct value for your region
end

config system interface
edit port1
set ip 10.220.64.120/24
set allowaccess ping https ssh http
end

config system route
edit 1
set device port1
set gateway 10.220.64.1
end

config system sql
set status remote
set database-name fp_fazlite # use whatever name that you want to give the database;
                             # use the same database name when you configure the collector VM
set database-type mysql # REQUIRED. If you omit this step, there will be problems
                             with generating the portal database and collector database.
set username fpc # use the database user name instead of fpc
set password xyz # use the password for the database user name
set server 10.220.64.121 # use the same IP address for the collector when you
                             configure it from the CLI
end

```

3. Check the NTP settings with the `show system ntp` command. Modify the settings for your environment if necessary. **NOTE:** The NTP source should be the same for all portal and collector VMs to synchronize the log time stamps across all devices.
4. Reboot the VM.
5. From the database console, check the FortiPortal version information:

```

mysql -u root -p
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 59741
Server version: 10.2.13-MariaDB-10.2.13+maria~xenial-log mariadb.org binary
distribution

```

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

```

MariaDB [(none)]> show databases;
+-----+
| Database          |
+-----+
| ftntpmcdb         |
| information_schema |
| mysql             |
| performance_schema |

```

```
| portal |
| portal_hcache |
+-----+
6 rows in set (0.00 sec)
```

```
MariaDB [(none)]> connect ftntpmcdb
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A
```

```
Connection id: 59845
Current database: ftntpmcdb
```

```
MariaDB [ftntpmcdb]> select DB_Version, Portal_Version from fpc_version;
+-----+-----+
| DB_Version | Portal_Version |
+-----+-----+
| 5.0.0      | 5.0.0_11      |
+-----+-----+
1 row in set (0.00 sec)
```

6. Log in to the portal using the user name `spuser` and the password `test123`:

<https://10.220.64.120/fpc/login>

Language English



FortiPortal

Login

[Forgot password](#)

Cloud Based Security Analytics and Management for Carriers and Managed Security Service Providers

The top banner is common for all of the pages (Dashboard, Customers, Devices, Admin, Audit).

7. Next, you need to set the portal database size available on the portal database server. Go to *Admin > Settings* to specify the *FPC Data Store Size*. For example, 1024 GB. (**NOTE:** The mail settings must also be configured during the first-time configuration.)
8. Next, upload the license file. Go to *Admin > System Info* and select *Upload License*.

9. After the license is uploaded, check that the license status is valid and the number of devices allowed is correct. (**NOTE:** The individual portal and collector VMs do not have serial numbers.)

Updating the SSL certificate file

If you are setting up a demo server, you can skip this procedure.

NOTE: You must upload the license first.

Use the following steps to import an SSL certificate for the FortiPortal VM.

From the Admin portal, select *Admin > System Info* to display information about the SSL certificate.

System Info page

The Certificate Information panel displays the certificate file name and private key file name.

From this panel, you can select and upload a new certificate and private key for the FortiPortal (using the PKCS#8 format).

NOTE: Do not use certificate import and export commands from the portal or collector VMs because they apply to the administration interface and not the FortiPortal application. The certificate signing request must be done on an external host and the signed certificate imported. For example:

```
openssl genrsa -des3 -out server.key 1024
cp server.key server.key.org
openssl rsa -in server.key.org -out server.key
openssl req -new -key server.key -out server.csr
openssl pkcs8 -topk8 -nocrypt -in server.key -out portal.key
openssl x509 -req -days 365 -in server.csr -signkey portal.key -out server.crt
```

After these steps are done, you need to upload the certificate file (*.crt file) and portal.key file from the FortiPortal UI (as instructed in the administration guide). After uploading the certificate file, restart your portal VM.

Collector installation

Use the following instructions to install and configure the first collector. You can add multiple collectors for more storage and an increased log rate.

1. Install the collector VM image using the `fpcvm64imageCollector.out.ovf.zip` file.
2. Configure the CLI settings. **NOTE:** The database server defined with the `config system sql` command is the portal database. The collector databases are configured from the FortiPortal application.

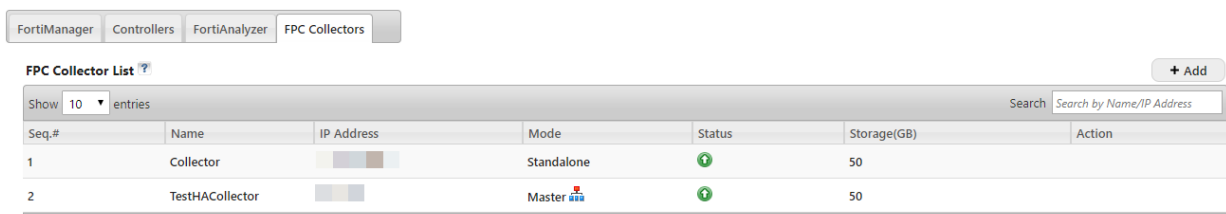
For example:

```
config system global
set hostname collector
set timezone 28
end
config system interface
edit port1
set ip 10.220.64.122/24
set allowaccess ping https ssh http
end
config system route
edit 1
set device port1
set gateway 10.220.64.1
end
config system sql
set status remote
set database-name portal
set database-type mysql
set password xyz
set server 10.220.64.121
set username fpc
end
```

3. Check the NTP settings with the `show system ntp` command. Modify the settings for your environment if necessary.
4. Reboot the collector.
5. Log in to the collector's management GUI to verify the installation:
<https://10.220.64.122:4443>

Adding the collector to the portal

1. Log in to the portal using a service-provider user account using the user name `spuser` and the password `test123`.
2. Go to *Devices > FPC Collectors* and then select *Add*.



The screenshot shows the FortiManager interface with the 'FPC Collectors' tab selected. Below the navigation tabs, there is a 'FPC Collector List' section with a search bar and a '+ Add' button. The table below lists the collectors:

Seq.#	Name	IP Address	Mode	Status	Storage(GB)	Action
1	Collector		Standalone		50	
2	TestHACollector		Master		50	

3. Enter a name and the IP address of the collector.

The screenshot shows a web-based configuration window titled "Add FPC Collector". It contains the following fields and values:

- * Name: collector
- * IP Address: 10.220.64.122
- Port Number: 443
- Mode: Standalone (dropdown menu)
- * Collector Username: admin
- Collector Password: [masked]
- Confirm Password: [masked]
- * DB IP Address: 10.220.64.123
- * DB Port Number: 3306
- * DB Username: fpc
- * DB Password: [masked]

At the bottom of the window are "Save" and "Cancel" buttons.

4. Select *Standalone* for the mode. If you are configuring a collector HA, select *Master*.
5. Enter the collector user name and password. By default, the user name is `admin`.
6. Enter the collector database IP address, user name, and password.
7. Enter the data storage size in GB.
8. Select **Save**.
9. Check the data store size again. It should be larger now that it includes the collector.

NOTE: The storage indicator increments by the collector database storage allocation. The overall storage indicator combines the portal database and all collector databases.

FortiManager configuration

You need to configure FortiManager to work with FortiPortal.

1. *The ADOM mode must be enabled for FortiManager to work with FortiPortal.* If needed, enable ADOMs and the advanced adom-mode on FortiManager so that you can add VDOMs on the same physical device to different ADOMs.

```
config system global
set adom-status enable
set adom-mode advanced
y
```

```
end
```

2. Create a portal user with read-and-write permission:

```
config system admin user
edit fpc
set profileid Super_User
set adom all_adoms
set policy-package all_policy_packages
set password fortinet
set rpc-permit read-write
next
end
```

3. The workspace mode must be enabled for FortiManager to work with FortiPortal.

```
config system global
set workspace-mode normal
end
```

4. Add your FortiManager device using the JSON port. You must poll FortiManager to see the device list. For more information about adding FortiManagers to the portal, see ["FortiManager devices"](#) on page 57.

FortiManager
Controllers
FortiAnalyzer
FPC Collectors

FortiManager List
+ Add

Show 10 entries
Search Search by FortiManager/IP Address:

FortiManager	IP Address	Mode	Status	Action
FMG001	10.106.6.221	Standalone	1	

Search Search by Device/Customer Name

Device	Status	Customer Name	Wireless
ADOM_52/FGVM010000094117/root	1		0
ADOM_52/FGVM010000094117/vd1	1		0
ADOM_52/FGVM010000094117/vd2	1		0
ADOM_52/FGVM010000094117/vd3	1		0
ADOM_52/FGVM010000094117/vd4	1		0
ADOM_52/FGVM010000094117/vd5	1		0
ADOM_52/FGVM010000094117/vd6	1		0
ADOM_52/FGVM010000094117/vd7	1		0
ADOM_52/FGVM010000094117/vd8	1		0
ADOM_52/FGVM010000094117/vd9	1		0

Showing 1 to 10 of 27 entries
Previous 1 2 3 Next

FMG002	172.30.71.142	Standalone	1
FMG003	10.106.6.231	Standalone	1
FMG004	10.106.6.232	Standalone	1

FortiAnalyzer configuration

You need to configure FortiAnalyzer to work with FortiPortal.

1. The ADOM mode must be enabled for FortiAnalyzer to work with FortiPortal. You must enable the interface permission `webservice` on FortiAnalyzer for the portal-facing interface.
2. You must allow remote procedure calls. Create an admin user for portal:

```
config system admin user
  edit <user_name>
    set rpc-permit read-write
  end
```

Additional setup tasks

After performing the basic installation, there are additional setup tasks to fully complete your configuration:

- To add additional collectors or to configure collector HA, see "[FortiPortal collectors](#)" on page 68.
- To add additional FortiManager devices, see "[FortiManager devices](#)" on page 57.
- To add wireless controllers, see "[AP controller devices](#)" on page 62.
- To add FortiAnalyzer devices, see "[FortiAnalyzer devices](#)" on page 65.
- To create an end customer, see "[Add or edit a customer](#)" on page 39.
- To create customer sites, see "[Customer sites](#)" on page 45.
- To create site administrators, see "[Customer Users](#)" on page 49.

Reset your password

Enter the Email ID associated with your user account.

Reset your password

Please enter your email address and we will send you a temporary password

* Email:

Send

Cancel

The system resets your password and sends you a temporary password by email.

NOTE: This command is available only when *Authentication Access* in Admin Settings is set to *Local*.

The default login credentials for the portal and collector are `admin` (for the user name) and no password.

Change Password

Enter your existing password and a new password. The default login credentials for the portal and collector are `admin` (for the user name) and no password.



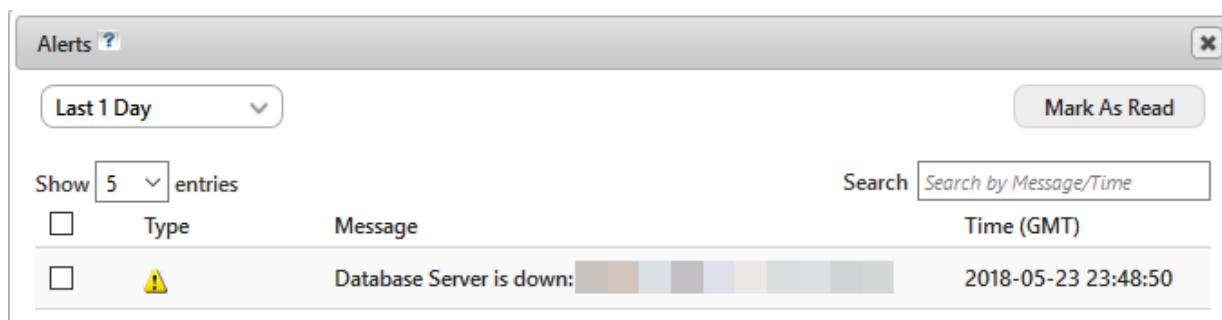
A screenshot of a 'Change Password' dialog box. The dialog has a title bar with the text 'Change Password' and a question mark icon. Below the title bar, there are three input fields, each preceded by a red asterisk: '* Old Password:', '* New Password:', and '* Confirm New Password:'. The 'New Password' field has a small yellow question mark icon to its right. At the bottom right of the dialog, there is a blue button labeled 'Change'.

The password change takes effect on your next log-in attempt.

NOTE: This command is available only when *Authentication Access* in Admin Settings is set to *Local*.

Alerts

The Alerts page displays a list of system alerts.



For each alert, the page displays the following

- **Type**—severity of the alert. Values include: Informational and Warning
- **Message**—text summary of the alert
- **Time**—time that the alert was raised. Times are all displayed in GMT time zone.

Page actions

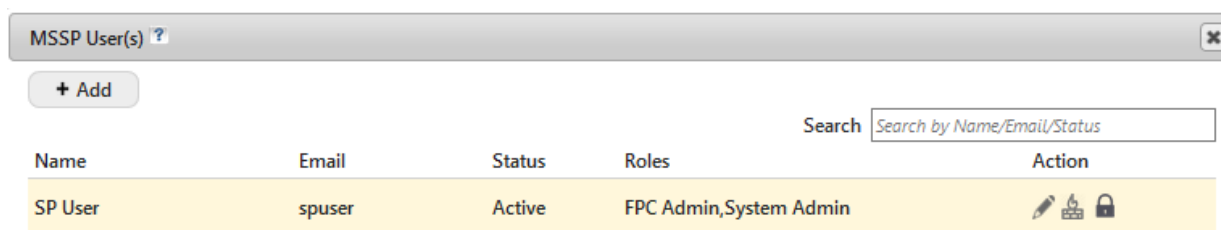
The Alerts page contains the following actions:




- **Filter**—filter the data (Last 60 Minutes, Last 1 day, Last 1 week)
- **Mark as Read**—mark selected alerts as read
- **Show x Entries**—use the drop-down selector to set the number of entries to display
- **Search**—enter text in the search box to search for alerts containing that text
- **Select**—select individual alerts, or select all alerts (select box in the column header)

Administrative users

Selecting the  icon on the top-right hand side displays the list of FortiPortal service provider administrators.

NOTE: These users are local users. The described commands are available only when *Admin Settings > Authentication Access* is set to *LOCAL*.



Name	Email	Status	Roles	Action
SP User	spuser	Active	FPC Admin, System Admin	  





Page actions

On this page, the following actions are available:

- *Add*—open a new page with the form to add an MSSP user
- *Search*—enter text to search for user names containing that text

Per-user actions

When you scroll over a entry in the users list, the following icons appear in the Action column:

-  —opens a new page with the form to edit the data for this user
-  —deletes the entry. (**NOTE: You cannot delete the default admin user.**)
-  —opens the Trusted Host list
-  —opens the Change Password dialog box

Create a user

1. From the MSSP User(s) page, select *Add*.

Add MSSP User
✕

* First Name:

* Last Name:

* Email:

Password Policy:
☒ Enable

* Password:

* Confirm Password:

Must Contain:

☒ Uppercase Letters
 ☒ Lowercase Letters
 ☒ Numbers (0-9)
 ☒ Special Characters

Minimum Length: (8-32 characters)

Address1:

Address2:

City:

State:

Country:

Zip:

Phone:

Fax:

Available Roles:

FPC Admin

System Admin

Admin Monitor

>

>>

<

<<

Selected Roles:

Status ☒ Active ☐ Disabled

Save

Cancel

2. Input the fields, as described in the table.

3. Select **Save**.

The following table describes the fields in the add/edit form:

Settings	Guidelines
First Name Last Name	Name of the administrator
Email	Email address of the administrator

Settings	Guidelines
Password Policy	Enable or disable. If enabled, you can set one or more of the following types of character that the password must contain: <ul style="list-style-type: none"> - Uppercase Letters - Lowercase Letters - Numbers (0-9) - Special Characters
Password Confirm Password	The administrator uses these credentials to access the customer portal. The password must meet the requirements set by the password policy.
Minimum Length	Select the minimum number of characters that a password must contain.
Address1 Address2 City State Country Zip	Business address for the administrator
Phone Fax	Phone and fax numbers
Available Roles	Roles that are available for this user type
Selected Roles	Selected roles for this user
Status	Select whether the MSSP user is <i>Active</i> or <i>Disabled</i> .

Trusted Hosts



If you enable Trusted Hosts as a global setting (see [Admin Settings](#)), the system enforces a configurable trust-host blocklist and whitelist for all admin and customer users.

You can also create a global trusted-host whitelist and subsequently open the list by selecting the *Trusted Host* option. The following figure shows a list with only the default entry:

Trusted Host

+ Add

Search

IP Start	Mask	Prefix	Action
0.0.0.0	0.0.0.0		
::		0	 

From the whitelist, you can edit/delete an existing trusted host, or add a trusted-host entry. The Add/Edit Trusted Host form contains the following fields:

Settings	Guidelines
IPv4	
IP Start	Start address for the range covered by this entry
Mask	Defines the range of IP addresses
IPv6	
IP Start	Start address for the range covered by this entry
Prefix	Defines the range of IP addresses covered by this entry

Admin user roles

The purpose of roles is to authorize each user to view and modify only the content that is required for that user. For example, a system administrator requires write access to the pages required for FortiPortal configuration, but does not need write access to the customer information.

Each role defines the access rights of the user to specific FortiPortal pages and components. The user may have read-write access to the content, or it may be hidden/read-only.

You can assign one or more roles to a user. For example, a user with Sys Admin and FortiPortal Admin roles is a "Super Admin," with read-write access to all Service Provider pages and all Customer Portal pages.

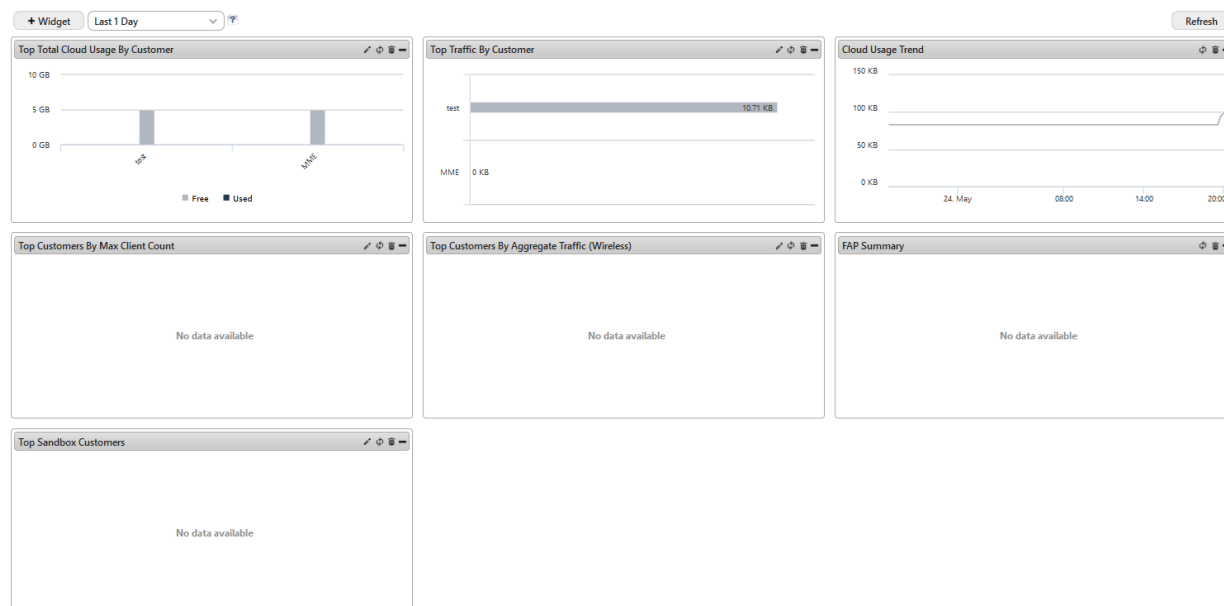
The system provides a set of default administrative roles. Using the [FortiPortal Roles](#) user interface, you can also create new roles or customize the default roles.

The following table describes the default roles for administrative users:

Settings	Guidelines
FPC Admin	The FortiPortal Admin role provides read-write access to all of the FortiPortal pages. but with read-only access to the collectors, administrator settings, system log, and themes. The FortiPortal Admin role also provides read-write access to the customer portal.
System Admin	The System Admin role provides read-only access to all of the FortiPortal pages. In addition, this role provides read-write access to the collectors, administrator settings, system log, and themes. The customer portal is hidden for the Sys Admin role.
Admin Monitor	The System Admin role provides read-only access to all of the FortiPortal admin portal and the customer portal.

Dashboard

The dashboard displays information about the FortiPortal and is organized as a set of widgets.



Actions available (at the top of the Dashboard page):

- **Widget**—add a widget to the dashboard
- **Filter**—filter the data based on time (last 60 minutes, last 1 day, last 7 days, or specify a custom filter)
- **Refresh**—refresh the display for all of the widgets on the page

The dashboard includes the following default widgets:

- Top Total Cloud Usage By Customer
 - Hover your cursor over each customer to view the detailed usage numbers
- Top Traffic By Customer
- Cloud Usage Trend
 - Hover your cursor over each customer to view the detailed numbers over the selected usage period
- Top Customers By Max Client Count
- Top Customers By Aggregate Traffic (Wireless)
 - Hover your cursor over each customer to view the detailed traffic numbers
- Fortinet Access Point (FAP) Summary
 - Select the pie chart to view a list of the FAPs that are up (select the left side) or FAPs that are down (select the right side of the pie chart)
- Top Sandbox Customers

The title bar on each widget provides the following controls:

- **Edit Settings**—opens a new page with a form to edit the widget details
- **Refresh**—refresh the widget display
- **Delete**—delete the widget

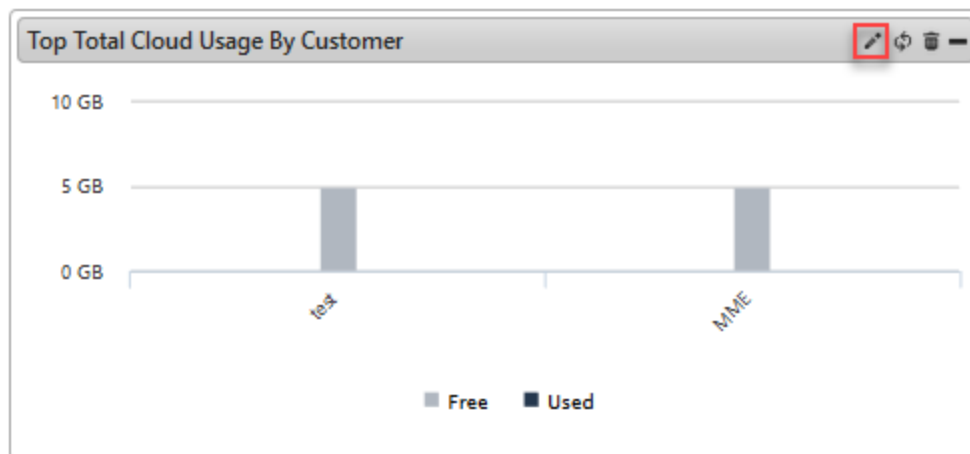
- *Collapse/Expand*—collapses the widget to display only the title bar
- Drag and drop—select and hold the title bar of the widget to change its position on the page

Initial data-aggregation delay

After FortiPortal begins to receive logs from the devices, you might experience a delay of up to 15 minutes before the aggregated data appears on the dashboard.

Setting the top N entries


From among the tools on the upper right on most widgets, you can use the *Edit Settings* icon to configure the widget to show the top N entries (5, 10, 15):



Select a number and select *Ok* to refresh the report.

Customers

The *Customers* page shows summary information for each customer (customer name, amount of storage allocated, and the percentage of their storage allocation that has been used).

Customer List 

[+ Add](#)

Show	10	entries	Search <input type="text" value="Search by Customer Name (or) Device/VDOM Name"/>			
Customer Name	Allocated Storage (GB)	Total Storage (%)	Portal Storage (%)	Collector Storage (%)	# FGT VDOM / FSA Devices	Action
MME	5.00	<input type="text" value="0.00"/>	<input type="text" value="0.00"/>	<input type="text" value="0.00"/>	2/0	
test	5.00	<input type="text" value="0.00"/>	<input type="text" value="0.00"/>	<input type="text" value="0.00"/>	1/0	

Page actions

On the Customers page, the following actions are available:

- *Show N entries*—filter the maximum number of customers to display in the page
- *Add*—open a new page with the form to add a customer. See ["Add or edit a customer"](#) on page 39.
- *Search*—enter text to search for customer names containing that text

Per-customer information

The system displays the following information for each customer:

Field	Description
Allocated Storage (GB)	Total amount of storage allocated for this customer
Total Storage (%)	Percentage of the total storage that the customer is currently using
Portal Storage (%)	Percentage of storage allocation (the customer is using) devoted to the portal
Collector Storage (%)	Percentage of storage allocation (the customer is using) devoted to the collector
# FGT VDOM / FSA Devices	<i>FGT VDOM Devices</i> —the number of FortiManager/FortiAP devices that are registered to this customer <i>FSA Devices</i> —the number of FortiSandbox devices that are registered to this customer

NOTE: The system displays the percentage of portal and collector storage allocations that the customer is using (not the percent of the total customer storage). These storage allocations are configurable in the add/edit customer forms.

Per-customer actions

Hovering over an entry in the customer table displays the following icons in the Action column:

- *Edit*—opens a new page with the form to [edit](#) the customer data. See "[Add or edit a customer](#)" on page 39.
- *Delete*—deletes this customer
- *Sites*—opens a pop-up window with a list of sites for this customer. See "[Customer sites](#)" on page 45.
- *User(s)*—opens a pop-up window with a list of users for this customer. See "[Customer Users](#)" on page 49.
- *Reports*—opens a pop-up window with a list of reports for this customer. See "[Reports](#)" on page 54.

When you select a customer name in the list, the system opens the customer portal for this customer (in a new tab).

Add or edit a customer

Selecting **Add** on the upper right of the Customer List displays a form for adding a new customer (fields in the form are blank). (Hovering over any entry in the Customer List display and selecting the **Edit Settings** icon displays the Edit Customer form, which is identical to the Add Customer form except that fields are set to the values for this customer.)

Add Customer ?

Customer Details * Customer Name: <input type="text"/> * Email: <input type="text"/> * First Name: <input type="text"/> * Last Name: <input type="text"/> Domains: <input type="text"/> * Locale: <input type="text" value="English"/> <input type="checkbox"/> Use MSSP Locale Attach Logo: <input type="button" value="Choose File"/> No file chosen			
Contact Information Address1: <input type="text"/> Address2: <input type="text"/> City: <input type="text"/> State: <input type="text"/> Country: <input type="text" value="Select a Country"/> Zip: <input type="text"/> Phone: <input type="text"/> Fax: <input type="text"/>			
Cloud Properties * Total Storage: <input type="text" value="5"/> GB Collector/FPC Storage Percentage: <input type="text" value="80/20"/> Analytics: <input checked="" type="radio"/> Enable <input type="radio"/> Disable * When Allocated Disk Space is Full: <input checked="" type="radio"/> Overwrite Oldest Logs <input type="radio"/> Stop Logging			
Others Trusted Hosts: <input checked="" type="radio"/> Enable <input type="radio"/> Disable Policy Installation Scheduler: <input type="text" value="None"/> <input checked="" type="checkbox"/> Display Storage <input checked="" type="checkbox"/> Display Site Policy Filter(s): <input type="text"/> Object Filter(s): <input type="text"/>			
Policy & Object Edit Permissions <input type="checkbox"/> All <input checked="" type="checkbox"/> AntiSpam <input checked="" type="checkbox"/> DLP Sensor <input checked="" type="checkbox"/> Firewall Address <input checked="" type="checkbox"/> Local Category <input checked="" type="checkbox"/> Service <input checked="" type="checkbox"/> Virtual IP <input checked="" type="checkbox"/> Application Control <input checked="" type="checkbox"/> DLP Filter RegEx <input checked="" type="checkbox"/> Zone Interface <input checked="" type="checkbox"/> Rating Overrides <input checked="" type="checkbox"/> User <input checked="" type="checkbox"/> Web Filtering <input checked="" type="checkbox"/> AntiVirus <input checked="" type="checkbox"/> Firewall Policy <input checked="" type="checkbox"/> IPS Sensor <input checked="" type="checkbox"/> Schedule <input checked="" type="checkbox"/> User group <input checked="" type="checkbox"/> Web Filter RegEx		Policy Tab Permissions <input type="checkbox"/> All <input checked="" type="checkbox"/> Central NAT <input checked="" type="checkbox"/> IPv6 DoS Policy <input checked="" type="checkbox"/> Interface Policy <input checked="" type="checkbox"/> DoS Policy <input type="checkbox"/> IPv6 Interface Policy <input type="checkbox"/> NAT64 Policy <input type="checkbox"/> IPv6 Policy <input type="checkbox"/> NAT46 Policy	
Widget Permissions Available Widgets: <input type="text" value="Search"/> Top Application Category Top Hostname By Traffic Top Region By Traffic Top Web Top Application By Traffic Top Spam Traffic History Top Traffic By Protocol		Adom Filter Permissions Available Adom Filters: <input type="text" value="Search"/> FMG001/ADOM_S2 FMG001/ADOM_S4 FMG001/ADOM_S6 FMG001/ADOM_DEV_S6 FMG001/Model_ADOM_S2 FMG002/FPC_ADOM_NEW FMG003/ADOM_S2 FMG003/ADOM_DEV2	

Save Cancel

To add or edit a customer:

1. Input the fields, as described in the following sections.
2. Select **Save**.

The Customer form comprises a number of panels. The following sections describe the fields in each panel.

Customer Details and Contact Information

These panels contains basic information about the customer:

Customer Details * Customer Name: <input type="text"/> * Email: <input type="text"/> * First Name: <input type="text"/> * Last Name: <input type="text"/> Domains: <input type="text"/> * Locale: <input type="text" value="English"/> <input type="checkbox"/> Use MSSP Locale Attach Logo: <input type="button" value="Browse..."/>			
Contact Information Address1: <input type="text"/> Address2: <input type="text"/> City: <input type="text"/> State: <input type="text"/> Country: <input type="text" value="Select a Country"/> Zip: <input type="text"/> Phone: <input type="text"/> Fax: <input type="text"/>			

Settings	Guidelines
Customer Details	
Customer Name	Customer's business name, which must be unique within this FortiPortal
First Name Last Name Email	Name and email of the primary customer contact
Domains	When using remote authentication, a customer may have users defined in more than one domain. Enter a domain and then select the green + button. The new domain appears in the list below the entry box.
Use MSSP Locale	Uses the MSSP locale (the language configured in Admin Settings).
Language	If you deselect the <i>Use MSSP Locale</i> checkbox, you can select a language for this customer. When a customer user logs in to the GUI, pages will display in this language. For Administrative users, the system will continue to use the language set in the Admin Settings.
Attach Logo	Download an image file for this customer's logo.
Contact Information	
Address1 Address2 City State Country Zip Phone Fax	Address fields and phone and fax numbers for this customer

Cloud Properties

This panel contains information about portal and collector storage for this customer.

Cloud Properties

Total Storage:

5

GB

Collector/FPC Storage Percentage:

80/20

Analytics

☒ Enable
 ☐ Disable

When Allocated Disk Space is Full:

☒ Overwrite Oldest Logs
 ☐ Stop Logging

Settings	Guidelines
Total Storage	Total number of GB of storage that this customer can use. The default value is 5 GB.
Collector/FPC Storage Percentage	Storage ratio for the collector database and portal database. By default, 80% of the storage allowance is allocated to the collector database, and 20% is allocated to the portal database.

Settings	Guidelines
Analytics	Enable or disable. If you disable analytics for a customer, the Dashboard, Views, and Reports pages will not be displayed to that customer. If you disable analytics when adding a new customer, the system allocates less storage space for the customer (1 GB instead of 5 GB).
When Allocated Disk Space is Full	Select one of two options: - Overwrite Oldest Logs - Stop Logging

Others

This panel allows you to configure other settings.

Settings	Guidelines
Trusted Hosts	Enable or disable trusted hosts for this customer. For additional information about trusted hosts, see "Customer Users" on page 49 .
Policy Installation Scheduler	Enables you to schedule automatic policy installation at a particular time (daily or weekly). All the pending policy updates will be installed at the configured schedule. If you select <i>None</i> , the installation scheduler is not invoked for this customer. If you select <i>Daily</i> , select the installation time. If you select <i>Weekly</i> , select the day and time for the policy installation.
Policy Filter(s)	Comments made in a policy can be added as filters in this section to hide the policy from customer users.
Object Filter(s)	Adding an object name to Object Filter(s) hides the object from the customer user. This allows MSSP users to hide any objects that need to be hidden from customers users.
Display Storage	Select to display the storage.
Display Site	Select to display the customer site.

Policy & Object Edit Permissions

This panel configures the policies and objects that a customer can modify.

NOTE: Policies and objects will not be visible to the customer in the customer web interface unless you select them.

For example, if you select *Web Filtering*, a web filter object will display in the object tree and a web filter column will display in the *Policy* tab:

Policy & Object Edit Permissions

<input type="checkbox"/> All	<input type="checkbox"/> Application Control	<input type="checkbox"/> AntiVirus
<input type="checkbox"/> AntiSpam	<input type="checkbox"/> DLP Filter RegEx	<input type="checkbox"/> Firewall Policy
<input type="checkbox"/> DLP Sensor	<input type="checkbox"/> Zone Interface	<input type="checkbox"/> IPS Sensor
<input type="checkbox"/> Firewall Address	<input type="checkbox"/> Rating Overrides	<input type="checkbox"/> Schedule
<input type="checkbox"/> Local Category	<input type="checkbox"/> User	<input type="checkbox"/> User group
<input type="checkbox"/> Service	<input type="checkbox"/> Web Filtering	<input type="checkbox"/> Web Filter RegEx
<input type="checkbox"/> Virtual IP		

Settings	Guidelines
Policy and Object Permissions	
Check boxes for Policies and Objects	<p>You can select edit permissions for <i>All</i> policies and objects or select edit permissions for individual policies and objects:</p> <p>AntiSpam, Application Control, AntiVirus, DLP Sensor, DLP Filter RegEx, Firewall Policy, Firewall Address, Zone Interface, IPS Sensor, Local Category, Rating Overrides, Schedule, Service, User, User group, Virtual IP, Web Filtering, and Web Filter RegEx</p>

Policy Tab Permissions

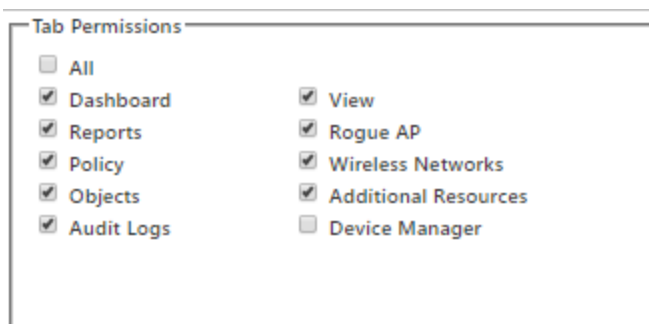
This pane determines which policy tabs are visible in the customer web interface. Select the check boxes for tabs that you want to make visible for this customer. Select *All* to make all of the tabs visible.

Policy Tab Permissions

<input type="checkbox"/> All	<input type="checkbox"/> IPv6 Interface Policy
<input type="checkbox"/> Central NAT	<input type="checkbox"/> NAT64 Policy
<input type="checkbox"/> IPv6 DoS Policy	<input type="checkbox"/> IPv6 Policy
<input type="checkbox"/> Interface Policy	<input type="checkbox"/> NAT46 Policy
<input type="checkbox"/> DoS Policy	

Tab Permissions

This pane determines the tabs that are visible in the customer web interface. Select the check boxes for tabs that you want to make visible for this customer. Select *All* to make all of the tabs visible.



Tab Permissions

<input type="checkbox"/> All	<input checked="" type="checkbox"/> View
<input checked="" type="checkbox"/> Dashboard	<input checked="" type="checkbox"/> Rogue AP
<input checked="" type="checkbox"/> Reports	<input checked="" type="checkbox"/> Wireless Networks
<input checked="" type="checkbox"/> Policy	<input checked="" type="checkbox"/> Additional Resources
<input checked="" type="checkbox"/> Objects	<input type="checkbox"/> Device Manager
<input checked="" type="checkbox"/> Audit Logs	

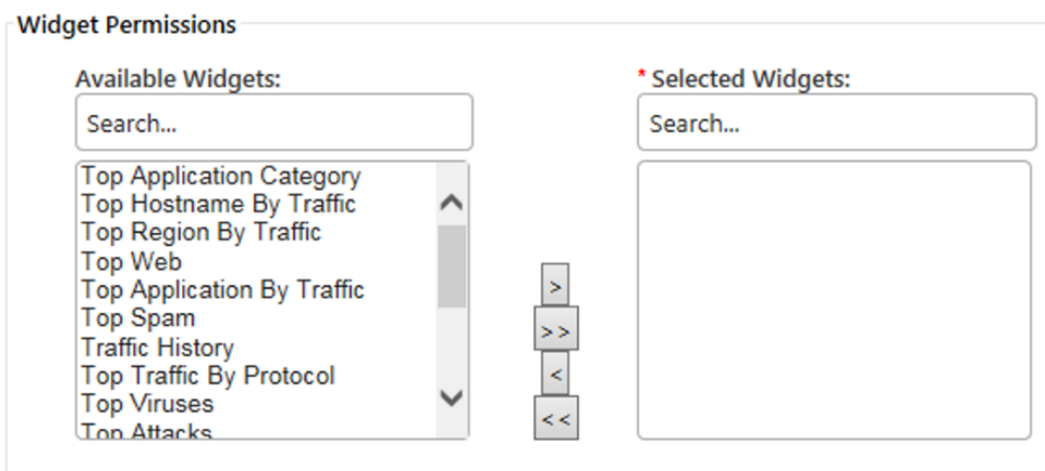
NOTE: You must include at least one of the following tabs: *Dashboard*, *Policy*, or *Objects*.

Widget Permissions

This pane determines the widgets that are available in the dashboard of the customer web interface.

NOTE: If you selected *Dashboard* in the Tab Permissions panel, you must select at least one widget for display in the dashboard.

Use the arrow keys to move the widgets from the left panel to the right panel (these widgets will appear in the dashboard for this customer). The double-arrow keys move the entire list.



Widget Permissions

Available Widgets:

Search...

Top Application Category
Top Hostname By Traffic
Top Region By Traffic
Top Web
Top Application By Traffic
Top Spam
Traffic History
Top Traffic By Protocol
Top Viruses
Top Attacks

>

>>

<

<<

*** Selected Widgets:**

Search...

ADOM Filter Permissions

This pane determines the devices that will be listed for a customer in drop-down menus of devices.

Use the arrow keys to move values from the left panel to the right panel.

Adom Filter Permissions**Available Adom Filters:**

fm/Adom4
fm/FortiSandbox
fm/root
fm/tenant-1
fm/tenant-2

**Selected Adom Filters:**

Customer sites

Hovering over an entry in the Customer List page “dynamically creates” a set of action icons:

Customer List ▼ + Add

Show 10 entries Search Search by Customer Name (or) Device/ADOM Name

Customer Name	Allocated Storage (GB)	Total Storage (%)	Portal Storage (%)	Collector Storage (%)	# FGT VDOM / FSA Devices	Action
MME	5.00	0.00	0.00	0.00	2/0	
test	5.00	0.00	0.01	0.00	1/0	

Selecting the *Sites* icon displays information about the customer sites. For each site, you see the name, devices, and email address of the site administrator:

Sites ? ✕

+ Add

Search

Name	Device	Email	Action
wireless	FPC_ADOM_NEW/FGVM010000101088/vd1...	wifi@site.com	

Page actions

The Sites page contains the following actions:

- *Add*—open a new page with the form to add a site
- *Search*—enter text to search for site names containing that text

Per-site actions

When you scroll over a entry in the Sites list, the following icons appear in the Action column:

Sites ? ✕

+ Add

Search

Name	Device	Email	Action
wireless	FPC_ADOM_NEW/FGVM010000101088/vd1...	wifi@site.com	

- *Wireless Network*—opens a pop-up window with a list of wireless networks for the selected site. See "[Wireless Networks](#)" on page 47.
- *Edit*—opens a new page with the form to add a site or edit existing site data
- *Delete*—deletes the selected site

Selecting **Add** displays the Add/Edit Site forms (selecting the **Edit Settings** icon under Actions displays an identical form with fields supplied):

Add Site

* Site Name:

* Contact Name:

* Email:

Phone:

Available Devices:

Search...

- ADOM_52/FGT700S/dmngmt-vdom
- ADOM_52/FGT700S/root
- ADOM_52/FGT700S/vd1
- ADOM_52/FGVM010000094117/root
- ADOM_52/FGVM010000094117/vd1
- ADOM_52/FGVM010000094117/vd2
- ADOM_52/FGVM010000094117/vd3
- ADOM_52/FGVM010000094117/vd4
- ADOM_52/FGVM010000094117/vd5

☐ Enable sandbox for all selected devices

Selected Devices:

Search...

> >> << <

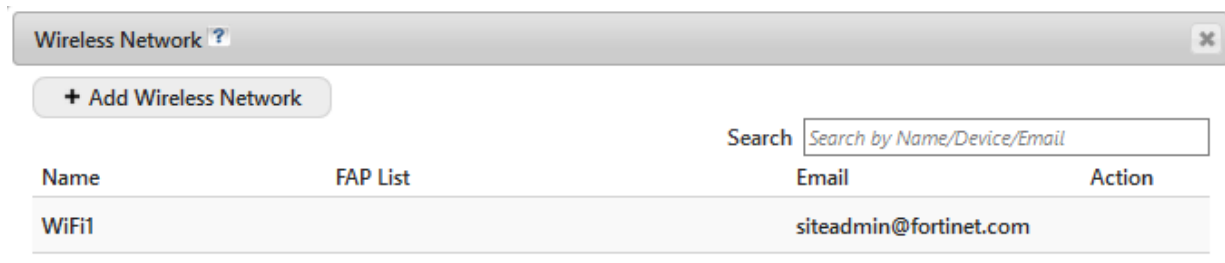
Save Cancel

The forms contain the following fields:

Settings	Guidelines
Site Name	Name for the Site, which must be unique across this customer's sites
Contact Name Email Phone	Name and email of the customer contact for this site
Available Devices	List of discovered FortiGate devices (with the format: ADOM/Device/VDOM Use the search box to filter the choices available.
Selected Devices	Select the devices to associate with this site. Ensure that you add only the devices with the correct ADOM for this customer. Use the search box to filter the choices available.
Enable sandbox for all selected devices	Set this option if you want to enable sandbox capability for all of the selected devices. NOTE: An extra license is required for each device that you enable with sandbox.

Wireless Networks

Selecting the *Wireless Network* icon on the Customer Sites page displays the Wireless Networks window for a given site. This window displays information about the site's wireless networks (network name, FAP list, email of the administrator):



The screenshot shows a window titled "Wireless Network" with a close button. Below the title bar is a button labeled "+ Add Wireless Network". To the right of this button is a search bar with the placeholder text "Search by Name/Device/Email". Below the search bar is a table with four columns: "Name", "FAP List", "Email", and "Action". The table contains one row with the following data: "WiFi1", (empty), "siteadmin@fortinet.com", and (empty).

Name	FAP List	Email	Action
WiFi1		siteadmin@fortinet.com	

From this window, you can add wireless networks to the site, edit a site, and edit the list of associated Fortinet Access Points.

Page actions

On this page, the following actions are available:

- *Add Wireless Network*—open a new page with the form to add a wireless network
- *Search*—enter text to search by network name, device or email

Selecting *Add Wireless Network* displays a form for adding a new network (fields in the form are blank).

Per-network actions

When you scroll over a entry in the wireless network table, the following icons appear in the Action column:

- *Edit*—opens a pop-up window with a form to edit the wireless network data
- *Delete*—deletes the selected wireless network

Selecting the *Edit* icon displays the Edit Wireless Network form, which is identical to the Add Wireless Network form except that the fields are filled:

Edit Wireless Network

* Wireless Network Name:

WiFi1

* Contact Name:

Site Admin

* Email:

siteadmin@fortinet.com

Phone:

Available Devices:

Search...

Selected Devices:

Search...

>

>>

<

<<

Save

Cancel

When you add or edit a wireless network, the form contains the following fields:

Settings	Guidelines
Wireless Network Name	Name for the wireless network
Contact Name	Name and email of the customer contact for this network
Email	
Phone	
Available Devices	Lists of discovered wireless AP devices Use the search box to filter the choices available.
Selected Devices	Select the wireless AP devices to associate with this network. Use the search box to filter the choices available.

Customer Users

Selecting the *User(s)* icon on the Customer List page displays the Customer User(s) page, which displays information about the local administrative users configured for this customer.

NOTE: These users are local. The described commands are available only when *Admin Settings > Authentication Access* is set to *Local*.




Page actions

On this page, the following actions are available:

- *Add*—open a new page with the form to add a user
- *Search*—enter text to search for user names containing that text

Per-user actions

When you scroll over a entry in the users list, the following icons appear in the Action column:

1. —opens a new page with the form to add/edit data for existing users
2. —deletes this user
3. —opens a new page with the form to add a trusted-host entry for this customer

Add or edit a customer user

Add Customer User

* First Name:

* Last Name:

* Email:

Password Policy:
☒ Enable

* Password:

* Confirm Password:

Must Contain:
☒ Uppercase Letters ☒ Lowercase Letters ☒ Numbers (0-9) ☒ Special Characters

Minimum Length:

8

(8-32 characters)

Address1:

Address2:

City:

State:

Country:

Select a Country

Zip:

Phone:

Fax:

Available Roles:

Search...

Customer Admin

>

>>

<

<<

Selected Roles:

Search...

Available Sites:

Search...

wireless

>

>>

<

<<

Selected Sites:

Search...

Status ☒ Active ☐ Disabled

Save

Cancel

The Add Customer User and Edit Customer User forms contain the following fields:

Settings	Guidelines
First Name Last Name	Name of the user
Email Password Confirm Password	Email and password for the user. The user will use these credentials to access the customer portal.
Password Policy	Enable or disable. If enabled, you can set one or more of the following types of character that the password must contain: <ul style="list-style-type: none"> - Uppercase Letters - Lowercase Letters - Numbers (0-9) - Special Characters
Minimum Length	Select the minimum number of characters that a password must contain.
Address1 Address2 City State Country Zip	Business address for the user
Phone Fax	Phone and fax number for the user
Available Roles	Roles that are available for this user type. You can specify multiple roles for a user.
Selected Roles	Selected roles for this user
Available Sites	Sites that are available for this user to access.
Selected Sites	Sites that this user can access. You can specify multiple sites for a user. If no site is selected, the user has access to all sites.
Status	Select whether the customer user is <i>Active</i> or <i>Disabled</i> .

Add a trusted host for a user

If you have enabled the Trusted Host option for this customer, the system creates a whitelist of trusted hosts for the customer users. The default entry in the whitelist is to allow all users, so you need to edit/delete this entry to create a valid whitelist.

Select the *Trusted Host* option to open the whitelist for this customer. The following figure shows a list with only the default entry:

Trusted Host
✕

+ Add

Search

IP Start	Mask	Prefix	Action
0.0.0.0	0.0.0.0		
::		0	

From the whitelist, edit/delete an existing trusted host, or add a trusted-host entry for this customer.

The Add Trusted Host and Edit Trusted Host forms contain the following fields:

Settings	Guidelines
IPv4	
IP Start	Enter the start address for the range covered by this entry.
Mask	Define the range of IP addresses covered by this entry.
IPv6	
IP Start	Enter the start address for the range covered by this entry.
:Prefix	Define the range of IP addresses covered by this entry.

Customer user roles

User roles enable you to authorize each customer user to view and modify only the content that is required for that user.

Each role defines the access rights of the user to specific Customer Portal pages and components. Content may be hidden from the user, read-only, or read-write access.

You can assign one or more roles to a user. For example, a user with Schedule Report Write and RunNow Report Execute roles will have read-write access to the Reports page and the RunNow page, and read-only access to the remaining pages and components for that customer.

The system provides a set of default customer user roles. You can also create new roles or customize the default roles using the Roles page. See ["Roles"](#) on page 94.

There are numerous default roles, but note the following common points:

- The Customer Monitor role provides read-write access to the pages that a user requires to administer the Customer Portal for that customer. Because this role is far-reaching, we recommend that you assign this role to a limited number of users.
- All of the customer roles provide read-write access to the dashboard.

- All of the "Read" roles provide read access to all of the customer pages (except that the Run Now Report page is hidden). In addition, the role allows read-only access to the resource that the role name specifies (such as Policy, Address Object, Schedule Object).
- Each of the "Write" roles provide read-only access to the same resources as the "Read" role, except that it also allows write access to the resource that the role name specifies (such as Policy, Address Object, Schedule Object).
- The RunNow Report Execute role allows access to the RunNow page, so that the user can run reports. On the report page, the *Run Now* button is hidden for users without this role.

NOTE: To provide a customer user with read-write access to a specific object or policy, you must set the corresponding write permission for this customer in the Customer data. Refer to *Policy and Object Permissions* in ["Add or edit a customer"](#) on page 39.

The following table describes the default role types that are available:

Role	Description
Customer Admin	Read-write access to the pages that an user requires to administer the Customer Portal for that customer
Schedule Report Read	Read access to the Report Definitions page
Schedule Report Write	Read access to the Report Definitions page and allows the user to add or edit a customer-defined report
Run Now Report Execute	Makes the Run Now button visible on the Reports page and enables the user to select a report and run it
Policy Read	Provides the user with read-only access to the policies
Policy Write	Provides the user with read-write access to the policies
Object Read	Provides the user with read-only access to the specified object type. Object types include: Address Object, Schedule Object, Anti Virus Object, Application Sensor Object , DLP Object, Email Filter Object, IPS Sensor Object, Web Filter Object.
Object Write	Provides the user with read-write access to the specified object type

Reports

The service provider can create reports for the customer. Similarly, the customer can also create reports. The ability (for a specific customer user) to create reports or run reports is based on the roles assigned to that user. For additional information, refer to ["Customer Users"](#) on page 49.

The *Reports* tab displays information about the reports that are available to this customer. From the selector on the top left of the page, you can select FortiPortal or FortiAnalyzer reports.

In the *Admin > Settings* page, you specify the maximum number of reports (*Max Reports Allowed*) that can be defined for this customer. This number includes customer-defined reports and reports added by the service provider. If you try to add a report beyond the maximum number for this customer, the system displays an error message.

FortiPortal reports

The following figure shows the *Reports > FortiPortal* page, which lists the user type and frequency for each report:

Created (GMT)	Date Range (GMT)	Report Name	Type	Action
2018-05-24 20:49:25	2018-05-23 20:49:25 / 2018-05-24 20:49:25	Report_MME_1527194965542.pdf	On Demand	

Page actions

The FortiPortal Reports page contains the following actions:

- **Select**—select FortiPortal or FortiAnalyzer
- **Range**—select the time period that the report will cover
- **Report Definitions**—define a report to run daily, weekly, or monthly
- **Run Now**—define a report to run immediately
- **Show *x* entries**—sets the number of entries that are displayed at once (10, 20, or 50)
- **Search**—enter text to search for within report names

Per-report actions

When you scroll over a entry in the reports list, the following icons appear in the Action column:

- **Download**—open or save the selected report
- **Delete**—deletes this report

The Add Report and Edit Report forms contain the following selections:

Settings	Guidelines
Report Name	Name for the report.
Frequency	Values include: Daily, Weekly, Monthly.
Available Reports Selected Reports	Use the arrow keys to create a list of selected reports by using the list of available reports. Use the search boxes to filter the choices available.
Available Sites Selected Sites	Use the arrow keys to create a list of selected sites from the list of available sites. If no sites are selected, the report is run for all sites. Use the search boxes to filter the choices available.
Language	Select the language for the report from the drop-down list.
No of Rows	Number of rows of data to include in the report.
From Email	Enter email address from which the report will be sent.
Email Text	Enter text for the body of the email.

FortiAnalyzer reports

The following figure shows the *Reports > FortiAnalyzer* page, which includes the reports that are available on all of the FortiAnalyzers devices associated with this FortiPortal.

Page actions

The FortiAnalyzer Reports page contains the following actions:

- **Select**—select one or more report (boxes) to assign or unassign to a customer
- **Range**—select the time period that the report will cover
- **Show *x* entries**—sets the number of entries that are displayed at once (8, 25, 50, or all)
- **Assign**—assigns the selected reports to this customer who can view a report or download a PDF of the content
- **Unassign**—removes the selected reports from this customer
- **Search**—enter text to search for within report names

NOTE: If you assign a report to a customer for a given ADOM, the other reports for that ADOM are unavailable to other customers.

Per-report actions

When you scroll over a entry in the reports list, the following icons appear in the Action column:

- *Assign*—assigns the selected reports to this customer who can view a report or download a PDF of the content
- *Unassign*—removes the selected reports from this customer

FortiManager devices

Go to *Devices > FortiManager* to see a list of FortiManager devices and the devices that they are managing:

FortiManager	Controllers	FortiAnalyzer	FPC Collectors
--------------	-------------	---------------	----------------

FortiManager List +				
Show 10 entries	Search <input type="text" value="Search by FortiManager/IP Address"/>			
FortiManager	IP Address	Mode	Status	Action
FMG001	10.106.6.221	Standalone		

Device	Status	Customer Name	Wireless
ADOM_52/FGVM010000094117/root			
ADOM_52/FGVM010000094117/vd1			
ADOM_52/FGVM010000094117/vd2			
ADOM_52/FGVM010000094117/vd3			
ADOM_52/FGVM010000094117/vd4			
ADOM_52/FGVM010000094117/vd5			
ADOM_52/FGVM010000094117/vd6			
ADOM_52/FGVM010000094117/vd7			
ADOM_52/FGVM010000094117/vd8			
ADOM_52/FGVM010000094117/vd9			

Showing 1 to 10 of 27 entries				Previous	1	2	3	Next
-------------------------------	--	--	--	----------	---	---	---	------

	FMG002	172.30.71.142	Standalone	
	FMG003	10.106.6.231	Standalone	
	FMG004	10.106.6.232	Standalone	

Page actions

On this page, the following actions are available:

- **Add**—open a new page to add a FortiManager
- **Show x entries**—sets the number of entries that are displayed at once (10, 20, 50, or All)
- **Search**—enter text to search for FortiManager names containing that text. You can also search by IP address.

Per-FortiManager actions

When you scroll over a entry in the FortiManager list, the following icons appear in the Action column:

- **Expand**—select the green + button to view a list of the devices managed by this FortiManager
- **Hide**—select the red - button to hide the devices managed by this FortiManager
- **Edit**—select to open a new page with the form to edit the FortiManager data
- **Delete**—select to delete the FortiManager

- *Poll*—select to poll the FortiManager
- *Show HA*—select to display the FortiManagers in this HA cluster
- *Change Password*—select to change the password for the FortiManager

FortiManager high availability (HA)

A FortiManager HA cluster consists of an active master unit, and up to four standby slave units. If the master unit becomes unavailable, one of the standby slaves will become the new master.

In most situations, the FortiPortal provides access to the master FortiManager in the HA cluster. Configuration changes in the master will be synchronized to the slave units. If no master exists, the FortiPortal provides read-only access to the slave units.

In the FortiManager table, the Mode includes the following values:

- *Standalone*—the FortiManager is independent of a high-availability cluster
- *Master*—the FortiManager is the master in a high-availability cluster
- *Slave*—the FortiManager is a slave in a high-availability cluster

Select the *HA* icon to display information about the FortiManagers in this HA cluster:

The screenshot shows a 'Cluster Information' dialog box with a search bar and a table of FortiManager units. The table has five columns: SN, Active, IP Address, Role, and Status. There are two rows of data. The first row shows a Master unit with SN FMG-VM0A15001610, IP 172.30.71.237, and a green arrow status. The second row shows a Slave unit with SN FMG-VM0A15000695, IP 172.30.71.141, and a green arrow status. An 'Ok' button is at the bottom right.

SN	Active	IP Address	Role	Status
FMG-VM0A15001610	✓	172.30.71.237	Master	↑
FMG-VM0A15000695	✗	172.30.71.141	Slave	↑

The Cluster Information page provides the following information for each FortiManager in the cluster:

Field	Description
FortiManager SN	Serial Number of the FortiManager
Active	Displays green arrow for an active FortiManager, or a gray x for an inactive FortiManager

Field	Description
IP Address	IP Address of the FortiManager
Role	Master or Slave
Status	Indicates whether the FortiManager is operational

Add a FortiManager

Assuming that you have already acquired the credentials for an admin user on the FortiManager (create a dedicated admin user for FortiPortal), do the following to add a FortiManager:

1. Select *Add*.
2. Input the fields, as described in the table in the next section.
3. Select *Save*.

When you add a FortiManager, the FortiPortal polls the FortiManager immediately to obtain information about its managed devices. The FortiPortal subsequently polls the FortiManager based on the configured polling frequency.

Edit a FortiManager

To edit the FortiManager:

1. Select the *Edit* button (in the Action column).
2. Input the fields, as described in the table below.
3. Select *Save*.

Edit FortiManager

* FortiManager Name:

FMG001

* IP Address:

* Admin Username:

admin

* Polling Frequency:

Daily

* ports:

JSON

443

Last Poll Time:

2018-05-23 17:19:41 (GMT)

Save

Cancel

The following table contains descriptions of the fields:

Field	Description
FortiManager Name	A name for the FortiManager. The name must be unique within this FortiPortal.
IP Address	IP address of the FortiManager
Admin Username	User name for a valid FortiManager administrative user
Polling Frequency	How frequent the FortiPortal will poll the FortiManager to update the devices information. If you set the frequency to No Polling , the FortiPortal will never poll the FortiManager. Valid values include Daily, Weekly, Monthly.
ports	Port number to use to connect with the FortiManager. The default for JSON is 443. The default for XML is 8080.
Last Poll Time	Read-only field. Indicates when the FortiPortal last polled this FortiManager device.

Manage FortiGate devices

Selecting the green + button on the FortiManager List page displays a list of the FortiGate devices managed by this FortiManager. The system displays an additional search box, for searching within the list of devices.

For each device, the system displays the following fields and action buttons.

- **Device**—name of the managed FortiGate device
- **Status**—status of the device
- **Customer Name**—the customer name
- **Wireless**—indicates whether this FortiGate device is functioning as a wireless controller. Selecting the icon displays the Edit Wireless Controllers page. Enter the admin user name and password for the FortiGate unit, and desired polling frequency. If the device is polled successfully, it will be added to the controller devices list.

NOTE: The system displays a cluster icon to represent a FortiGate cluster. Hovering over the icon displays the list of individual FortiGate units in the cluster (see the figure below):

Search <small>Search by Device/Customer Name</small>			
Device	Status	Customer Name	Wireless
AratiAdom/FWF90D3Z14002442/vd7			
KamranADOM/FWF90D3Z14002442/vd3			
PravinADOM/FWF90D3Z14002442/vd4			
root/FWF90D3Z14002442/vd5			
SasiADOM/FWF90D3Z14002442/vd1			
SureshADOM/FWF90D3Z14002442/vd2			
VenkataADOM/FGT60D4613055589/root		Customer2	
VenkataADOM/FGT60D4613055589/vd1		Customer1	
VenkataADOM/FGT60D4613055589/vd2		Customer3	
VenkataADOM/FOSVM/root			

to 10 of 16 entries

Previous 1 2 Next

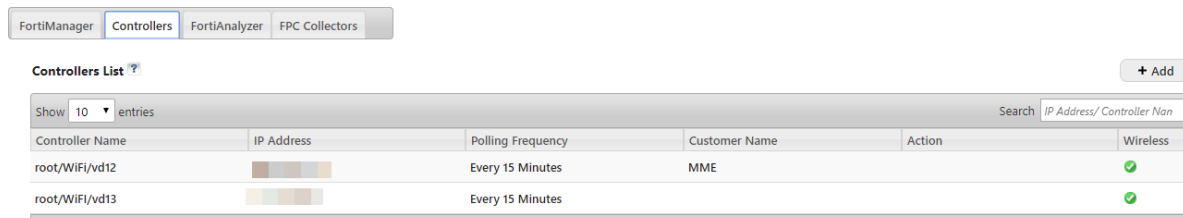
Cluster Information

FGT60D4613051234

FGT60D4613054767

AP controller devices

Go to *Devices > Controllers* to see a list of wireless AP controllers. (In the FortiPortal solution, the wireless controllers are FortiGate devices.)



Controller Name	IP Address	Polling Frequency	Customer Name	Action	Wireless
root/WiFi/vd12		Every 15 Minutes	MME		✓
root/WiFi/vd13		Every 15 Minutes			✓

The list displays the controller name (with ADOM and VDOM), the IP address, and the polling frequency for each controller. Polling frequency determines how often the FortiPortal will poll the device for any updated data.



For the FortiPortal to collect the data for this device, the SSID name and interface name (configured on the FortiGate or FortiWireless controller) must match precisely.

Page actions

On this page, the following actions are available:

- *Add*—open a new page with the form to add a controller device
- *Show x entries*—sets the number of entries that are displayed at once (10, 20, 50, or 100)
- *Search*—enter text to search for controller names containing that text

Per-controller actions

When you scroll over an entry in the controller table, the following icons appear in the Action column:

- *Edit*—opens a pop-up window with a form to edit the controller data
- *Delete*—deletes the selected controller
- *Change Password*—select to change the password for the controller

Wireless icons:

- *Wireless*—indicates whether this FortiGate is acting as a wireless controller. Select the icon to toggle the status
- *Attention*—wireless connectivity status of the FortiGate unit

Edit a controller

To edit the controller :

1. Select the *Edit* button (in the Action column).
2. Change the fields as needed; see the field descriptions in the table.
3. Select *Save*.

The following figure shows the Edit Wireless Controllers form:

Edit Wireless Controllers

* Controller Name: WiFi

* ADOM: root

* VDOM: vd12

* IP Address:

* Serial Number: FWF90D1212122222

* Admin Username: admin

* Port Number: 443

* Polling Frequency: Every 15 Minutes ▼

Save Cancel

The following table contains descriptions of the fields:

Settings	Guidelines
Controller Name	Name for the controller. The combination of controller name and VDOM must be unique within this FortiPortal
ADOM	Administrative domain to which this controller belongs

Settings	Guidelines
VDOM	Virtual domain to which this controller belongs
IP Address	IP address of the controller
Serial Number	Serial number of the controller
Admin Username	User name for the controller user assigned to this FortiPortal
Port Number	Destination port number for polling messages. The default is 443.
Polling Frequency	How often the FortiPortal will poll the controller to update the device information. Values range from every 15 minutes to every 24 hours.

FortiAnalyzer devices

Go to *Devices > FortiAnalyzer* to see a list of FortiAnalyzers. When you add a FortiAnalyzer device to the FortiPortal, you make the reports on that FortiAnalyzer available to customers. Refer to the [Customer Reports](#) page. The list displays the FortiAnalyzer name, the IP address, and the status for each FortiAnalyzer:

Name	IP Address	Status	Action
FAZ	10.106.6.211		

Prerequisites

Before you add a FortiAnalyzer device, use the FortiAnalyzer CLI to set the following configuration values:

1. Set permission level for the user to login via Remote Procedure Call (RPC).

```
config system admin user
  edit <the admin user name assigned to the FortiPortal>
    set rpc-permit read-write
```

2. Set port1 (assuming it is connected to the FortiPortal) to allow web service access.

```
config system interface
  edit port1
    set allowaccess https http ping telnet snmp webservice
    aggregator fortimanager
```

Page actions

On this page, the following actions are available:

- *Add*—open a new page with the form to add a FortiAnalyzer device
- *Show x entries*—sets the number of entries that are displayed at once (10, 20, 50, or All)
- *Search*—enter text to search with FortiAnalyzer names

Per-FortiAnalyzer actions

When you scroll over an entry in the FortiAnalyzer table, the following icons appear in the Action column:

- *Edit*—opens a pop-up window with a form to edit the FortiAnalyzer data
- *Delete*—deletes the selected FortiAnalyzer
- *Poll*—polls the FortiAnalyzer to obtain the most recent data

- *View*—displays a list of FortiAnalyzer reports
- *Change Password*—select to change the password for the FortiAnalyzer

Edit a FortiAnalyzer

To edit the FortiAnalyzer:

1. Select the *Edit* button (in the Action column).
2. Change the fields as needed; see the field descriptions in the table.
3. Select *Save*.

The following figure shows the form to edit a FortiAnalyzer:

Edit FortiAnalyzer: FAZ [X]

* Name:

* IP Address:

* Admin Username:

* ports: JSON ▼

Polling Frequency: Daily

Last Poll Time: 2018-05-23 19:22:37 (GMT)

The following table contains descriptions of the fields:

Settings	Guidelines
Name	Name for the FortiAnalyzer. The combination of FortiAnalyzer name and VDOM must be unique within this FortiPortal.
IP Address	IP address of the FortiAnalyzer
Admin Username	User name for the FortiAnalyzer user assigned to this FortiPortal

Settings	Guidelines
ports	Port number to use to connect with the FortiAnalyzer. The default for JSON is 443. The default for XML is 8080.
Polling Frequency	How often the FortiPortal will poll FortiAnalyzer to update the device information. The default value is one day. The polling frequency is not configurable.
Last Poll Time	The most recent time that FortiPortal polled FortiAnalyzer.

View FortiAnalyzer reports

When you select the *View* icon for a FortiAnalyzer in the list, FortiPortal opens a pop-up window:

FortiAnalyzer Reports

Show 8 entries

Search

Name	Customer Name
ADOM_50/360-Degree Security Review	
ADOM_50/Admin and System Events Report	
ADOM_50/Application Risk and Control	
ADOM_50/Bandwidth and Applications Report	
ADOM_50/Client Reputation	
ADOM_50/Cyber Threat Assessment	
ADOM_50/Data Loss Prevention Detailed Report	
ADOM_50/Detailed Application Usage and Risk	

Showing 1 to 8 of 262 entries

Previous

1

2

3

4

5

33

Next

Ok

FortiPortal collectors

Go to *Devices > FPC Collectors* to see a list of the FortiPortal collector devices. For each collector, the list displays its IP address, mode, status, and database storage size:

FortiManager
Controllers
FortiAnalyzer
FPC Collectors

FPC Collector List
+ Add

Show 10 entries
Search Search by Name/IP Address

Seq.#	Name	IP Address	Mode	Status	Storage(GB)	Action
1	Collector		Standalone		50	
2	TestHACollector		Master		50	

Page actions

On this page, the following actions are available:

- *Add*—open a new page with the form to add a collector
- *Show x entries*—sets the number of entries that are displayed at once (10, 20, 50, or 100)
- *Search*—enter text to search for in collector names

Collector high availability (HA)

A collector HA cluster consists of an active master unit and one or more standby slave units.

The portal controls the collector HA cluster and polls the collectors (using HTTPS) every 30 seconds to check that they are active. If the master unit becomes unavailable, the portal automatically selects (using a simple round-robin algorithm) which standby slave becomes the new master without the need for human intervention. There is no loss of data between when the master unit becomes unavailable and the new master becomes active because all collectors receive the same data.

When a new master unit becomes active, you will see the following alert:

```
New Primary was elected: CollectorNN[xxx.xxx.xxx.xxx]
```

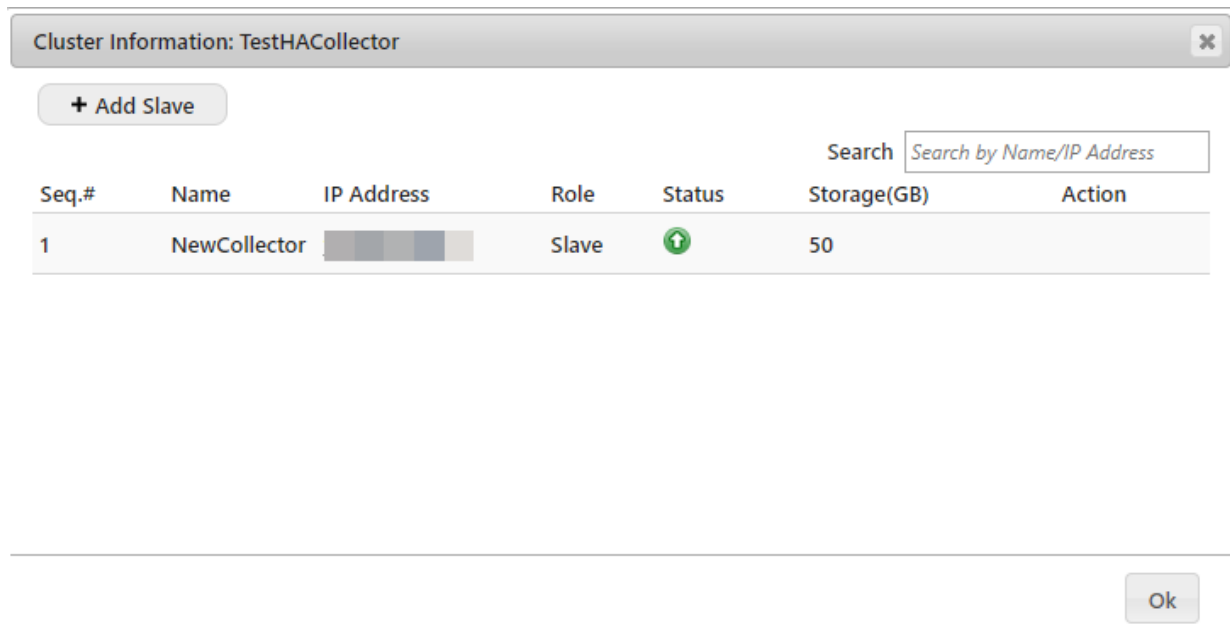
For example:

```
New Primary was elected: Collector10[192.15.50.108]
```

Use the following steps to create a high-availability cluster:

1. Add one collector with the mode set to *Master*.

2. Select the *HA* icon in the mode column to open the Cluster Information window.



The screenshot shows a window titled "Cluster Information: TestHACollector". Inside the window, there is a button labeled "+ Add Slave". Below this is a search bar with the placeholder text "Search by Name/IP Address". A table displays the cluster information with the following columns: Seq.#, Name, IP Address, Role, Status, Storage(GB), and Action. The table contains one row with the following data: Seq.# 1, Name NewCollector, IP Address (represented by a greyed-out box), Role Slave, Status (indicated by a green up arrow icon), Storage(GB) 50, and Action (empty). At the bottom right of the window is an "Ok" button.

Seq.#	Name	IP Address	Role	Status	Storage(GB)	Action
1	NewCollector		Slave	↑	50	

3. Select *Add Slave* to create the slave.

Add a FortiPortal collector

You need to add at least one collector to the FortiPortal:

1. Select *Add*.
2. Edit the fields, as shown in the following figure. The fields are described in the table at the end of this section.
3. Select *Save*.

Add FPC Collector

* Name:

* IP Address:

Port Number:

443

Mode:

Standalone

* Collector Username:

Collector Password:

Confirm Password:

* DB IP Address:

* DB Port Number:

3306

* DB Username:

* DB Password:

Save

Cancel

Per-collector actions

When you scroll over a entry in the FPC Collector List, the following icons appear in the Action column:

- *Edit*—opens a new page with the form to edit the collector data (page is identical to Add FPC Collector except for the supplied values)
- *Delete*—deletes the selected collector
- *Change Password*—select to change the password for the collector

Edit a collector

1. Select the *Edit* button (in the Action column).
2. Change the fields as needed; the fields are described in the table.
3. Select *Save*.

Settings	Guidelines
Name	Name for this collector. Each collector name must be unique within a FortiPortal.
IP Address	IP address of the collector
Port Number	Port number for connecting with the collector. Default value is 443.
Mode	Standalone or Master
Collector Username	Valid user name for the collector
Collector Password Confirm Password	Password for the collector user.
DB IP Address	The IP address of the collector MySQL database.
DB Port Number	Port number for the collector database. Default value is 3306.
DB Username	Valid user name for the collector database.
DB Password Confirm Password	Password for the collector database user.
Data Store Size	The amount of database storage (in GB) to reserve for this collector.

Admin settings

Go to *Admin > Settings* to change the general administrative settings for the FortiPortal. The following figure shows the settings page (with authentication set to local):

The following table describes the settings:

Settings	Guidelines
Administrative Settings	
FPC Data Store Size	Amount of database storage (in GB) to reserve for the portal DB
Session Timeout	Timeout for user sessions on the Administrative or Customer web interfaces. The default is 30 minutes. The range is 15-3240 minutes.
Trusted Hosts	Select <i>Enable</i> or <i>Disable</i> . When enabled, you can create a whitelist of originating IP subnetworks; only log-in requests from these subnetworks will be allowed. The system also provides a blacklist, for blocking rogue log-in attempts.
Email Settings	
SMTP Server	URL of the SMTP serve from which FortiPortal sends emails
Email From	Email address. Emails sent from FortiPortal will originate from this address.

Settings	Guidelines
Port	Email server port. The default value is 25.
Authentication	Enable or disable authentication. If you enable authentication, enter a user name and password. You can use special characters in the user name.
User Authentication	
Authentication Access	<p>Select <i>Local</i> or <i>Remote</i>.</p> <p>If the authentication access is local, the service provider and customer user log-in credentials are checked in the local user databases. With the local option, you must add an SP user entry for each administrative user, and a customer user for each end-customer user.</p> <p>If the authentication access is remote, the service provider and customer user log-in credentials are checked in the remote RADIUS server or FortiAuthenticator user database. Local users can still be used when remote authentication is selected. See "Remote authentication using FortiAuthenticator" on page 74, "RADIUS server configuration " on page 76, and "Remote authentication—SSO " on page 80.</p> <p>NOTE: When you change the authentication configuration from local to remote or from remote to local, you must restart the FortiPortal.</p>
Other	
Store Aggregation Data for	Length of time (in days) that the system will save the aggregation data. Values include: 30, 60, 90, or 180 days. The default is 30 days.
Store Report Data for	Length of time (in days) that the system will save report data. Values include: 30, 60, 90, 180, or 365 days. The default is 180 days.
Load Balancer Domain/IP Address	Load balancer IP address or domain name, if you have configured multiple instances of the Apache Tomcat server.
Load Balancer Port	Load balancer port number (required if you specified a load balancer IP address, not required for a domain name). The default value is 443.
Max Reports Allowed	Maximum number of reports that can be defined for this customer. This number includes customer-defined reports and also any reports that the service provider has defined for this customer.
Alert Email From	Alert emails will be sent from this email address.
Alert Email To	Alert emails will be sent to this email address.

Settings	Guidelines
Language	Desired language (default, English) If you change the language, save the settings and log out. The change takes effect upon subsequent logins.
Time Zone	Select the appropriate time zone to use.
TLS/SSL Versions	Select which TLS/SSL versions are used.
Remote Log Server	
Primary Server	Primary log server IP address
Primary Port	Primary log server port number (mandatory if server address supplied)
Secondary Server	Secondary log server IP address
Secondary Port	Secondary log server port number (mandatory if server address supplied)

Remote authentication using FortiAuthenticator

When you select *Authentication Access > Remote*, the system displays additional settings to configure.

NOTE: If you change the authentication configuration from local to remote or from remote to local, you must restart FortiPortal.

The screenshot shows the 'User Authentication' configuration page. Under 'Authentication Access', 'Remote' is selected. The 'Remote Server' dropdown is set to 'FortiAuthenticator'. The 'Allow Service Provider Usernames without Domain' option is set to 'Disable'. There are input fields for 'Remote Server Key', 'Remote Server IP Address', 'Remote Server Port', and 'Remote Server User'. A 'Domains' list is also visible with a green plus icon for adding domains and a red minus icon for removing them.

The following table describes the remote authentication fields:

Settings	Guidelines
Remote Server	Select <i>FortiAuthenticator</i> , <i>RADIUS</i> , or <i>SSO</i> .
Allow Service Provider Usernames without Domain	Enable or disable. If you enable this field, the user can enter the user ID without a domain qualifier, and the system will try to authenticate the user credentials in each of the domains until a match is found.
Remote Server Key	Secret key for REST API requests

Settings	Guidelines
Remote Server IP Address	IP address of the authentication server
Remote Server Port	Port for the authentication server (default is 443)
Remote Server User (FortiAuthenticator only)	Administrator user name for the authentication server. This user must have sufficient permission to initiate REST API requests.
Domains	The service provider may allow administrative users to be defined in more than one domain. Enter a domain and then select the + button. The new domain appears in the list below the entry box.

If you select *RADIUS* as the remote server, the system displays the View Roles icon beside the *Remote Server* drop-down list. Select this icon to configure the RADIUS roles ("[RADIUS Roles](#)" on page 77).

Radius Roles ?

+ Add

Search

Name	Role Type	FPC Roles	Action
No data available			

RADIUS server configuration

Configure the following in the RADIUS server:

1. Add the following vendor-specific attributes to the Fortinet dictionary file:

Fortinet-Fpc-User-Role
Fortinet-Fpc-Tenant-Identification

For example, if you are using FreeRADIUS:

```
#
#           Fortinet's VSAs
#

VENDOR          Fortinet          12356

BEGIN-VENDOR    Fortinet
ATTRIBUTE       Fortinet-Group-Name      1  string
ATTRIBUTE       Fortinet-Client-IP-Address  2  ipaddr
ATTRIBUTE       Fortinet-Vdom-Name        3  string
ATTRIBUTE       Fortinet-Client-IPv6-Address  4  octets
ATTRIBUTE       Fortinet-Interface-Name    5  string
ATTRIBUTE       Fortinet-Access-Profile    6  string
ATTRIBUTE       Fortinet-Fpc-User-Role     40 string ###add this
ATTRIBUTE       Fortinet-Fpc-Tenant-Identification 41 string ###add this

#
# Integer Translations
#

END-VENDOR Fortinet
```

2. To configure FortiPortal roles in the RADIUS server, use the following vendor-specific attribute. You can specify multiple roles by using comma-separated values:

VENDORATTR 12356 Fortinet-Fpc-User-Role 40 string

(NOTE: A user will not be able to login to FortiPortal if the roles are not configured on the RADIUS server.)

3. To configure which sites will use RADIUS authentication, use the following vendor-specific attribute. You can specify multiple sites by using comma-separated values. If no sites are specified, users have access to all sites.

VENDORATTR 12356 Fortinet-FPC-Tenant-User-Sites 42 string

4. Specify the customer identification, which is used to map a particular user to a customer profile. The RADIUS server will send one of the domain names specified in the *Domains* field of the customer settings, in the value of

the new VSA.

VENDORATTR Fortinet-FPC-Tenant-Identification 41 string

RADIUS Roles

Selecting the *View Roles* (that is, role mapping) icon adjacent to the Remote Server field on the Settings page displays the RADIUS Roles page. Here, you can configure the mapping between FortiPortal roles and RADIUS roles. For each RADIUS role, the page displays the role type (Service Provider or Customer) and a list of FortiPortal roles that map to the RADIUS role.

RADIUS Roles ?

+ Add

Search

Name	Role Type	FPC Roles	Action
No data available			

The RADIUS Roles page contains the following actions:

- *Add*—open a new page with the form to add a RADIUS role (see immediately below)
- *Search*—enter text to search for RADIUS role names containing that text

Add Radius Role

* Role Name:

* Role Type:

Service Provider

* Available FPC Roles:

Search...

FPC Admin
System Admin
Admin Monitor
Customer Admin

Selected FPC Roles:

Search...

>

>>

<

<<

Save

Cancel

When you scroll over a entry in the RADIUS role list, the following icons appear in the Action column:



- *Edit*—opens a new page with the form to edit an existing RADIUS role (see below)
- *Delete*—deletes the selected RADIUS role

Radius Roles ?

✕

+ Add

Search

Name	Role Type	FPC Roles	Action
New FortiPortal Ad...	Service Provider	FPC Admin	 

The Add Radius Role and Edit Radius Role forms contain the following fields:

Settings	Guidelines
Role Name	Names the RADIUS role. The name must match a role name in the RADIUS server.
Role Type	Service Provider or Customer
Available FPC Roles:	Lists of available FortiPortal roles Use the search box to filter the choices available.
Selected FPC Roles	Selects the FortiPortal roles to associate with this RADIUS role Use the search box to filter your selected choices.

Remote authentication—SSO

If you select SSO as the remote server type, the system displays additional settings to configure:

The screenshot shows the 'Settings' page for SSO authentication. The 'Remote Server' is set to SSO. The 'Authentication' section shows 'Local' and 'Remote' options, with 'Remote' selected. The 'Domains' section shows a list of domains. The 'Other' section shows 'Store Aggregation Data for' and 'Store Report Data for' settings. The 'Remote Log Server' section shows 'Primary Server' and 'Secondary Server' settings.

For SSO, FortiPortal supports Service Provider - initiated or Identity Provider - initiated SAML authentication. The following table describes the SSO authentication fields:

Settings	Guidelines
Remote Server	SSO
Allow Service Provider Usernames without Domain	Enable or Disable. If you enable this field, the user can enter their user ID without a domain qualifier, and the system will try to authenticate the user credentials in each of the domains until a match is found.
SSO IDP Entity URL	IDP Entity URL (ID) or URN for SAML provided by IDP server
IDP Sign On Service Endpoint URL	Endpoint URL for IDP (Post/Redirect) provided by IDP Server
SSO Application ID	SSO application provided by IDP
SSO Audience URL	URL used for audience within assertion (format: <code>https://<FPC_PORTAL>/fpc/saml/SSO</code>)
Role Attribute	Attribute parameter name that maps to the corresponding role in FortiPortal

Settings	Guidelines
Tenant Identification Attribute	<p>Introduced with FortiPortal Version 3.2.1, this attribute specifies a 'string' value that FortiPortal uses under SSO to map a user to a specific customer.</p> <p>This feature works similar to the Tenant Identification Attribute in RADIUS, except that in SSO, FortiPortal allows you to configure the name of the attribute on the Administration Settings page.</p> <p>If you configure "My Customer Id" as the attribute value, FortiPortal expects the following in the authentication response from the SSO server:</p> <pre><My Customer Id>Fortinet</My Customer Id></pre> <p>where Fortinet is the value returned by the SSO server. This value must have been supplied to the "Domains" field in the Customer Add/Edit screen.</p> <p>For a RADIUS server, the Tenant Identification Attribute value is a Fortinet Vendor Attribute value. The server will send "Fortinet" in the authentication response.</p> <p>NOTE: FortiPortal treats the attribute values from either RADIUS or SSO server equally.</p>
Domains	<p>The service provider may allow administrative users to be defined in more than one authentication domain.</p> <p>Enter a domain, URL, or URN and then select the + button. The new domain appears in the list below the entry box.</p>
SSO Error URL	(Optional) Error URL provided by IDP
IDP Logout Service Endpoint	(Optional) IDP logout URL provided by IDP
SSO Certificate	Certificate provided by IDP used by SP to decrypt the signed response
Site Attribute	<p>Attribute parameter name that specifies which sites the customer user can access.</p> <p>For example, an attribute name of "site" might have the values "site1" and "site2". A customer user assigned to "site" would be able to access "site1" and "site2".</p> <pre><saml:Attribute Name="site" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"> <saml:AttributeValue xsi:type="xs:string">site1</saml:AttributeValue> <saml:AttributeValue xsi:type="xs:string">site2</saml:AttributeValue> </saml:Attribute></pre>

For troubleshooting SSO configuration, FortiPortal provides the following URL for the SPUSER to authenticate locally (even if the system configured for SSO remote authentication):

`https://<Portal>/fpc/adminuser/login`

Frequently asked questions (FAQs) about SSO configuration

How can I map the role (permission) for the IDP server user to the FortiPortal roles (permission)?

Use the following procedure to select the Role Type to make sure the right roles are mapped:

1. When you select the remote server, select the icon beside the drop-down list (Selection UI element).
A new window opens.
2. Select the *Add* button.
3. In the *Add SSO role* window, select the *Role Name* (This name must be an SSO role.) and then select *Available FPC Roles*.
4. Save your changes.

How can role mapping help maintain secured access to the system?

The MSSP administrator can create different roles on FortiPortal by going to *Admin > Roles* and selecting *Add*. The administrator can create a read-only role or a read-write role for a specific UI page or for a specific action. After a role is created, the role can be associated with an existing role on the IDP server. When users are authenticated, the role coming from the IDP server is mapped to a role in FortiPortal and the appropriate permissions are provided to the user.

The advantage of using this mapping is that the MSSP administrator does not need to change anything on the IDP server exclusively for FortiPortal.

How can I create custom roles (permission groups) on the FortiPortal unit?

The FortiPortal unit allows the MSSP to create different permission groups so that users can be mapped with appropriate permissions. For example, the MSSP user (spuser) can create a read-only permission group and a read-write permission group for different UI objects. These permission groups are created for the MSSP level, as well as the customer level.

These permission groups can be created from the UI by going to *Admin > Roles*.

Name	Role Type	Permissions	Type	Action
Admin Monitor	Service Provider	Dashboard-Read-Write,Customers-Read-Only,Users-Read-Only,Sites-Read-Only,WifiNetwork...	Default	
Customer Admin	Customer	CustomerDashboard-Read-Write,FortiView-All-Read-Only,WirelessNetwork-Read-Only,Cust...	Default	

What is the Tenant Identification attribute?

The FortiPortal unit has a multitenancy feature. This feature helps different types of users to access the system. The MSSP (service provider) users are typically administrators of the system; by using roles/permission groups, these users can have a different type of access. Other types of users are customer (MSSP customer) users.

During authentication, the FortiPortal unit needs to identify whether each user is an MSSP or a customer so that the correct user interface is loaded. The FortiPortal uses the user domain name to identify which interface should be loaded. For example if the user name in the IDP response is abc@domain.com, the system extracts

domain.com from the user name field and checks if this domain is mapped to a customer or an MSSP. Based on that mapping, the system displays the correct UI.

When the domain name is missing in the user name field, the system uses the Tenant ID attribute to map the users as customer or MSSP.

How can the Tenant ID attribute help maintain the appropriate privileged access to the system?

The Tenant ID attribute value is processed from the IDP response, and the value is mapped with the domain name field in the FortiPortal unit. For example, if tenant ID is `map_id`, FortiPortal gets the respective value for the `map_id` attribute from the SAML response and maps that value with the domain name listed in Add Customer or Edit Customer form or the *Admin > Settings* form. If the value matches with the customer domain name, the user is granted access to the customer. If the value matches with the domain name in the *Admin > Settings* form, FortiPortal loads the administrator UI.

How can I add a domain name to the customer?

A unique domain name identifies the customer. You can add the domain name to the customer when you add a customer or edit the customer. In the Add/Edit Customer window, there is the Domains field. Enter the domain name and select the + icon to add the name to the domain list.

NOTE: The MSSP can add more than one domain to a customer.

How can I add a domain name for a server provider?

After you select SSO/FortiAuthenticator/RADIUS as a remote server in the Settings page, you will see an option for the domain field.

SNMP

Enable the SNMP agent on the FortiPortal device so it can send traps to and receive queries from the computer that is designated as its SNMP manager. This allows for monitoring the FortiPortal with an SNMP manager.

SNMP has two parts—the SNMP agent that is sending traps, and the SNMP manager that monitors those traps. The SNMP communities on monitored FortiGate devices are hard coded and configured by the FortiPortal system—they are not user configurable.

The FortiPortal SNMP implementation is read-only. SNMP v1, v2c, and v3 compliant SNMP manager applications, such as those on your local computer, have read-only access to FortiPortal system information and can receive FortiPortal system traps.

SNMP agent

The SNMP agent sends SNMP traps originating on the FortiPortal system to an external monitoring SNMP manager defined in a SNMP community. Typically an SNMP manager is an application on a local computer that can read the SNMP traps and generate reports or graphs from them.

The SNMP manager can monitor the FortiPortal system to determine if it is operating properly, or if there are any critical events occurring. The description, location, and contact information for this FortiPortal system will be part of the information an SNMP manager will have — this information is useful if the SNMP manager is monitoring many devices, and it will enable faster responses when the FortiPortal system requires attention.

To configure the SNMP agent, go to `https://<portal_or_collector_IP_address>:4443` and log in using the default VM credentials (`admin` and no password). Then go to *System Settings > Advanced > SNMP*.

SNMP

SNMP Agent

☐ Enable

Description

Location

Contact

Apply

SNMP v1/v2c

Community Name	Queries	Traps	Enable	Action
public			<input checked="" type="checkbox"/>	

SNMP v3

User Name	Security Level	Notification Hosts	Queries	Action
-----------	----------------	--------------------	---------	--------

The following information and options are available:

SNMP Agent	Select to enable the SNMP agent. When the SNMP agent is enabled, it sends FortiPortal SNMP traps.
Description	Optionally, type a description of this FortiPortal system to help uniquely identify this unit.

Location	Optionally, type the location of this FortiPortal system to help find it in the event it requires attention.
Contact	Optionally, type the contact information for the person in charge of this FortiPortal system.
SNMP v1/2c	The list of SNMP v1/v2c communities added to the FortiPortal configuration.
Create New	<p>After you enable the SNMP agent, select <i>Create New</i> to add a new SNMP community. If the SNMP agent is not enabled, this button is not displayed.</p> <p>For more information, see "SNMP" on page 84.</p>
Community Name	The name of the SNMP community.
Queries	The status of SNMP queries for each SNMP community. The enabled icon indicates that at least one query is enabled. The disabled icon indicates that all queries are disabled.
Traps	The status of SNMP traps for each SNMP community. The enabled icon indicates that at least one trap is enabled. The disabled icon indicates that all traps are disabled.
Enable	Enable or disable the SNMP community.
Delete	Delete the selected SNMP community or communities.
Edit	Edit the selected SNMP community.
SNMP v3	The list of SNMPv3 users added to the configuration.
Create New	<p>After you enable the SNMP agent, select <i>Create New</i> to add a new SNMP user. If the SNMP agent is not enabled, this button is not displayed.</p> <p>For more information, see "SNMP v3 users" on page 89.</p>
User Name	The user name for the SNMPv3 user.
Security Level	The security level assigned to the SNMPv3 user.
Notification Hosts	The notification host or hosts assigned to the SNMPv3 user.
Queries	The status of SNMP queries for each SNMP user. The enabled icon indicates queries are enabled. The disabled icon indicates they are disabled.
Delete	Delete the selected SNMP user or users.
Edit	Edit the selected SNMP user.

SNMP v1/v2c communities

An SNMP community is a grouping of equipment for network administration purposes. You must configure your FortiPortal to belong to at least one SNMP community so that community's SNMP managers can query the FortiPortal system information and receive SNMP traps from it.



These SNMP communities do not refer to the FortiGate devices the FortiPortal system is managing.

Each community can have a different configuration for SNMP traps and can be configured to monitor different events. You can add the IP addresses of up to eight hosts to each community. Hosts can receive SNMP device traps and information.

To create a new SNMP community:

1. Go to *System Settings > Advanced > SNMP* and enable the SNMP agent.
2. In the SNMP v1/v2c section, select *Create New* in the toolbar.
The New SNMP Community pane opens.

New SNMP Community

Community Name

Hosts:

IP Address	Interface	Delete
<input type="button" value="Add"/>		

Queries:

Protocol	Port	Enable
v1	<input type="text" value="161"/>	<input checked="" type="checkbox"/>
v2c	<input type="text" value="161"/>	<input checked="" type="checkbox"/>

Traps:

Protocol	Port	Enable
v1	<input type="text" value="162"/>	<input checked="" type="checkbox"/>
v2c	<input type="text" value="162"/>	<input checked="" type="checkbox"/>

SNMP Event	Enable
Interface IP changed	<input checked="" type="checkbox"/>
Log disk space low	<input checked="" type="checkbox"/>
CPU Overuse	<input checked="" type="checkbox"/>
Memory Low	<input checked="" type="checkbox"/>
System Restart	<input checked="" type="checkbox"/>
CPU usage exclude NICE threshold	<input checked="" type="checkbox"/>
High licensed device quota	<input checked="" type="checkbox"/>
High licensed log GB/day	<input checked="" type="checkbox"/>
Log Alert	<input checked="" type="checkbox"/>
Log Rate	<input checked="" type="checkbox"/>
Data Rate	<input checked="" type="checkbox"/>

3. Configure the following options and then select *OK* to create the community.

Community Name Enter a name to identify the SNMP community. This name cannot be edited later.

Hosts	<p>The list of hosts that can use the settings in this SNMP community to monitor the FortiPortal system.</p> <p>When you create a new SNMP community, there are no host entries. Select <i>Add</i> to create a new entry that broadcasts the SNMP traps and information to the network connected to the specified interface.</p>
IP Address	<p>Enter the IP address and netmask of an SNMP manager.</p> <p>By default, the IP address is 0.0.0.0 so that any SNMP manager can use this SNMP community.</p>
Interface	Select the interface that connects to the network where this SNMP manager is located from the drop-down list. This must be done if the SNMP manager is on the Internet or behind a router.
Delete	Select the delete icon to remove this SNMP manager entry.
Add	Select to add another entry to the Hosts list. Up to eight SNMP manager entries can be added for a single community.
Queries	Enter the port number (161 by default) the FortiPortal unit uses to send v1 and v2c queries to the FortiPortal unit in this community. Enable queries for each SNMP version that the FortiPortal system uses.
Traps	Enter the Remote port number (162 by default) the FortiPortal unit uses to send v1 and v2c traps to the FortiPortal unit in this community. Enable traps for each SNMP version that the FortiPortal unit uses.
SNMP Event	<p>Enable the events that will cause SNMP traps to be sent to the community.</p> <ul style="list-style-type: none"> • Interface IP changed • Log disk space low • CPU Overuse • Memory Low • System Restart • CPU usage exclude NICE threshold • RAID Event (only available for devices that support RAID) • Power Supply Failed (only available on supported hardware devices) • High licensed device quota • High licensed log GB/day • Log Alert • Log Rate • Data Rate

To edit an SNMP community:

1. Go to *System Settings > Advanced > SNMP*.
2. In the SNMP v1/v2c section, select *Edit* in the same row as the community that you want to edit.

The Edit SNMP Community pane opens.

3. Edit the settings as required and then select *OK* to apply your changes.

To delete an SNMP community:

1. Go to *System Settings > Advanced > SNMP*.
2. In the SNMP v1/v2c section, select *Delete* in the row of the community that you need to delete.
3. Select *OK* in the confirmation dialog box to delete the selected community or communities.

SNMP v3 users

The FortiPortal SNMP v3 implementation includes support for queries, traps, authentication, and privacy. SNMP v3 users can be created, edited, and deleted as required.

To create a new SNMP user:

1. Go to *System Settings > Advanced > SNMP* and enable the SNMP agent.
2. In the SNMP v3 section, select *Create New* in the toolbar.
The New SNMP User pane opens.

New SNMP User

User Name

Security Level

No Authentication, No Privacy ▾

Notification Hosts

Queries

☐ Enable
 Port

161

SNMP Event

SNMP Event	Enable
Interface IP changed	<input checked="" type="checkbox"/>
Log disk space low	<input checked="" type="checkbox"/>
CPU Overuse	<input checked="" type="checkbox"/>
Memory Low	<input checked="" type="checkbox"/>
System Restart	<input checked="" type="checkbox"/>
CPU usage exclude NICE threshold	<input checked="" type="checkbox"/>
High licensed device quota	<input checked="" type="checkbox"/>
High licensed log GB/day	<input checked="" type="checkbox"/>
Log Alert	<input checked="" type="checkbox"/>
Log Rate	<input checked="" type="checkbox"/>
Data Rate	<input checked="" type="checkbox"/>

OK

Cancel

3. Configure the following options and then select **OK** to create the community.

User Name	The name of the SNMP v3 user.
Security Level	The security level of the user. Select one of the following: <ul style="list-style-type: none"> <i>No Authentication, No Privacy</i> <i>Authentication, No Privacy</i>: Select the <i>Authentication Algorithm</i> (SHA1 or MD5) and enter the password. <i>Authentication, Privacy</i>: Select the <i>Authentication Algorithm</i> (SHA1 or MD5), the <i>Private Algorithm</i> (AES or DES), and enter the passwords.
Notification Hosts	The IP address or addresses of the host. Select the add icon to add multiple IP addresses.
Queries	Select to enable queries and change the port number if needed. The default port is 161.

SNMP Event	<p>Enable the events that will cause SNMP traps to be sent to the SNMP manager.</p> <ul style="list-style-type: none"> • Interface IP changed • Log disk space low • CPU Overuse • Memory Low • System Restart • CPU usage exclude NICE threshold • RAID Event (only available for devices that support RAID) • Power Supply Failed (only available on supported hardware devices) • High licensed device quota • High licensed log GB/day • Log Alert • Log Rate • Data Rate
------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

To edit an SNMP user:

1. Go to *System Settings > Advanced > SNMP*.
2. In the SNMP v3 section, select *Edit* in the row of a user that you want to edit.
The Edit SNMP User pane opens.
3. Edit the settings as required and then select *OK* to apply your changes.

To delete an SNMP user:

1. Go to *System Settings > Advanced > SNMP*.
2. In the SNMP v3 section, select *Delete* in the row of the user that you want to delete
3. Select *OK* in the confirmation dialog box to delete the selected user or users.

SNMP MIBs

You can obtain the MIB files from Customer Service & Support (<https://support.fortinet.com>):

- /FortiAnalyzer/v5.00/Core MIB/FORTINET-CORE-MIB.mib
- /FortiAnalyzer/v5.00/5.2/5.2.0/FORTINET-FORTIMANAGER-FORTIANALYZER-MIB.mib

To be able to communicate with the SNMP agent, you must include all of these MIBs into your SNMP manager. Generally your SNMP manager will be an application on your local computer. Your SNMP manager might already include standard and private MIBs in a compiled database that is ready to use. You must add both MIBs to this database.

SNMP traps

Fortinet devices share SNMP traps, but each type of device also has traps specific to that device type. For example, FortiPortal units have FortiPortal specific SNMP traps. To receive Fortinet device SNMP traps, you

must load and compile the FORTINET-CORE-MIB.mib file into your SNMP manager.

Traps sent include the trap message as well as the unit serial number (fnSysSerial) and host name (sysName). The Trap Message column includes the message that is included with the trap, as well as the SNMP MIB field name to help locate the information about the trap.

Trap message	Description
ColdStart, WarmStart, LinkUp, LinkDown	Standard traps as described in RFC 1215.
CPU usage high (fnTrapCpuThreshold)	<p>CPU usage exceeds the set percent. This threshold can be set in the CLI using the following commands:</p> <pre>config system snmp sysinfo set trap-high-cpu-threshold <percentage value> end</pre>
CPU usage excluding NICE processes (fnSysCpuUsageExcludedNice)	<p>CPU usage excluding NICE processes exceeds the set percentage. This threshold can be set in the CLI using the following commands:</p> <pre>config system snmp sysinfo set trap-cpu-high-exclude-nice-threshold <percentage value> end</pre>
Memory low (fnTrapMemThreshold)	<p>Memory usage exceeds 90 percent. This threshold can be set in the CLI using the following commands:</p> <pre>config system snmp sysinfo set trap-low-memory-threshold <percentage value> end</pre>
Log disk too full (fnTrapLogDiskThreshold)	Log disk usage has exceeded the configured threshold. Only available on devices with log disks.
Temperature too high (fnTrapTempHigh)	A temperature sensor on the device has exceeded its threshold. Not all devices have thermal sensors. See manual for specifications.
Voltage outside acceptable range (fnTrapVoltageOutOfRange)	Power levels have fluctuated outside of normal levels. Not all devices have voltage monitoring instrumentation.
Power supply failure (fnTrapPowerSupplyFailure)	Power supply failure detected. Available on some devices that support redundant power supplies.
Interface IP change (fnTrapIpChange)	The IP address for an interface has changed. The trap message includes the name of the interface, the new IP address and the serial number of the Fortinet unit. You can use this trap to track interface IP address changes for interfaces with dynamic IP addresses set using DHCP or PPPoE.

Fortinet and FortiPortal MIB fields

The Fortinet MIB contains fields reporting current Fortinet unit status information. The following tables list the names of the MIB fields and describe the status information available for each one. You can view more details about the information available from all Fortinet MIB fields by compiling the FORTINET-CORE-MIB.mib file into your SNMP manager and browsing the Fortinet MIB fields.

System MIB fields:

MIB field	Description
fnSysSerial	Fortinet unit serial number.

Administrator accounts:

MIB field	Description
fnAdminNumber	The number of administrators on the Fortinet unit.
fnAdminTable	Table of administrators.
fnAdminIndex	Administrator account index number.
fnAdminName	The user name of the administrator account.
fnAdminAddr	An address of a trusted host or subnet from which this administrator account can be used.
fnAdminMask	The netmask for fnAdminAddr.

Custom messages:

MIB field	Description
fnMessages	The number of custom messages on the Fortinet unit.

MIB fields and traps:

MIB field	Description
fmModel	A table of all FortiPortal models.

Roles

Go to *Admin > Roles* to see role information (type and permissions) for each FortiPortal role:

Settings	Roles	System Log	Theme	System Info	Trusted Hosts	Additional Resources
----------	-------	------------	-------	-------------	---------------	----------------------

Roles List					+ Add
Show	10	entries	Search <input type="text" value="Search by Name/Permissions"/>		
Name	Role Type	Permissions	Type	Action	
Admin Monitor	Service Provider	Dashboard-Read-Write,Customers-Read-Only,Users-Read-Only,Sites-Read-Only,WifiNetwork...	Default		
Customer Admin	Customer	CustomerDashboard-Read-Write,FortiView-All-Read-Only,WirelessNetwork-Read-Only,Cust...	Default		

Page actions

The Roles page contains the following actions:

- *Add*—open a new page with the form to add a role
- *Search*—enter text to search for role names containing that text

Per-role actions

When you scroll over a entry in the roles list, the following icons appear in the Action column:

- *Edit*—opens a new page with the form to edit an existing role
- *Delete*—deletes the selected role

Selecting the + *Add* button displays the Add Role form which contains the following fields (selecting the *Edit Settings* icon under *Actions* displays an identical form with the fields entered):

Add Role ✕

* Role Name:

* Role Type:

Service Provider ▼

Available Permissions:

Search...

Dashboard-Read-Write
Customers-Read-Only
Customers-Read-Write
Users-Read-Only
Users-Read-Write
Sites-Read-Only
Sites-Read-Write
WifiNetworks-Read-Only
WifiNetworks-Read-Write

>
>>
<
<<

Selected Permissions:

Search...

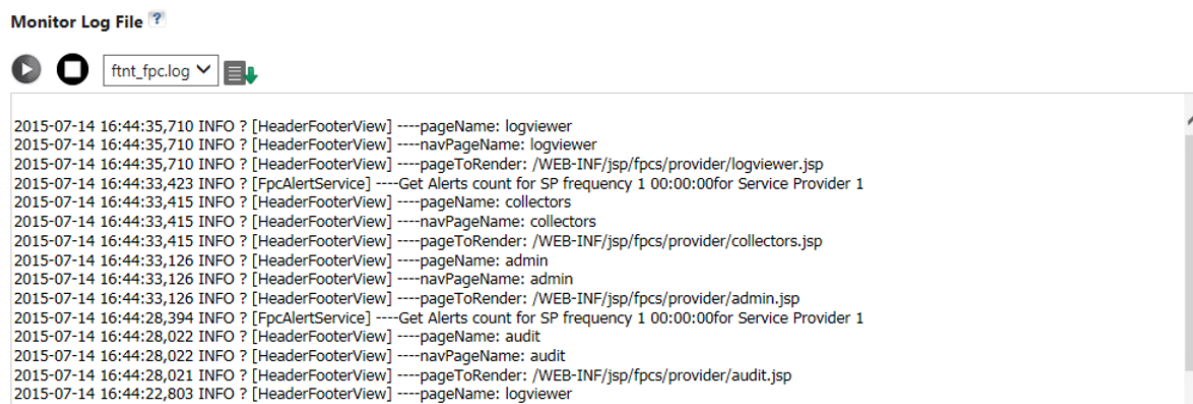
Save

Cancel

Settings	Guidelines
Role Name	Name for the role, which must be unique for this customer
Role Type	Service Provider or Customer
Available Permissions:	List of available FortiPortal permissions Use the search box to filter the choices available.
Selected Permissions	FortiPortal permissions to associate with this role Use the search box to filter your selected choices.

System Log

Go to *Admin > System Log* to monitor and download a set of system logs:



Page actions

- **Start**—starts to display the system logs
- **Stop**—stops the system logs
- **Download**—exports the captured system logs in a file

Initial log-aggregation delay

After FortiPortal starts to receive the logs, there might be a delay of up to 15 minutes before the aggregated data appears on the dashboard.

Theme

FortiPortal provides a default UI theme that is applied to the Administrative Web Interface and the Customer Portal Interface. The Theme page provides configuration fields that allow you to customize this theme. Configuration changes apply to both user interfaces (Administrative and Customer portal).

Custom theme options

You can configure customizations such as:

- Select a predefined color scheme.
- Create a custom color scheme.
- Define custom URLs and text fields.
 - URLs such as contact information and privacy policy.
 - Custom text for your company name, service name and service description.
- Upload custom images.
 - images for the log-in page and page banner

All of the custom fields are optional. Blank fields will be ignored.

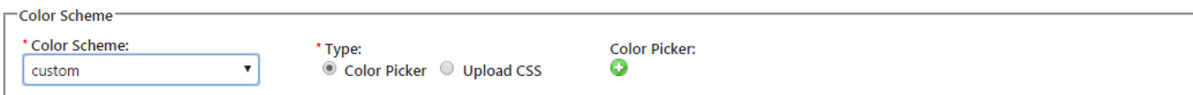
Select a predefined color scheme

From the Color Scheme panel of the *Theme* tab, select one of the predefined schemes. This scheme takes effect when you select *Save*.

Create a custom color scheme

Define a custom color scheme by selecting colors in a *Color Picker* or by changing the FortiPortal CSS file. Although you can switch between the two methods, these systems are independent. For example, changes made in *Color Picker* do not modify the colors in the CSS file.

The following figure shows the Color Scheme panel after you select to customize a scheme:



Using the color picker

To use the color picker to create a custom color scheme, select *custom* in the Color Scheme selector, and select the green *Color Picker* icon. This opens the Add Custom Color Scheme form.

Edit Custom Color Scheme

Global Settings
 Font Family:

Background Color Settings
 Page: Page Header: Page Footer:
 Button: Widget Header: Progress Bar:

Font/Text Color Settings
 Page: Page Header: Page Footer:
 Button: Widget Header: Login Screen:

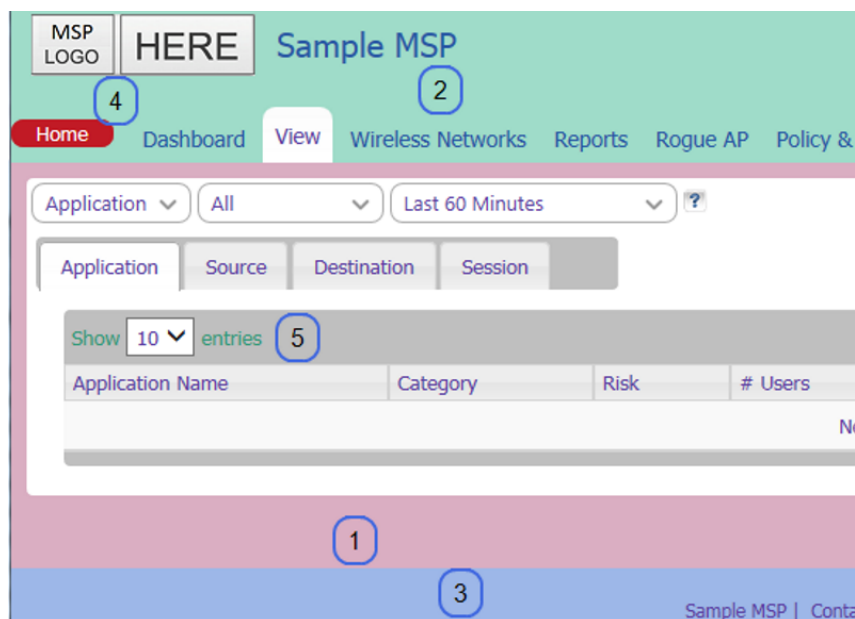
Chart Series Color Settings
 Series #1: Series #2: Series #3:
 Series #4: Series #5: Series #6:

The form is divided into the following sections:

- Global Settings
 - Select the Font Family to use for all text on the site.
- Background Color Settings
 - Select the colors for various page elements.
- Font/Text Color Settings
 - Select the text colors for various text fields.
- Chart Series Color Settings
 - Color selection for each slice in a pie chart.

Changes take effect when the theme is saved successfully.

The following figure shows the page elements that have custom background colors and text colors (see the table below for descriptions of the callouts):

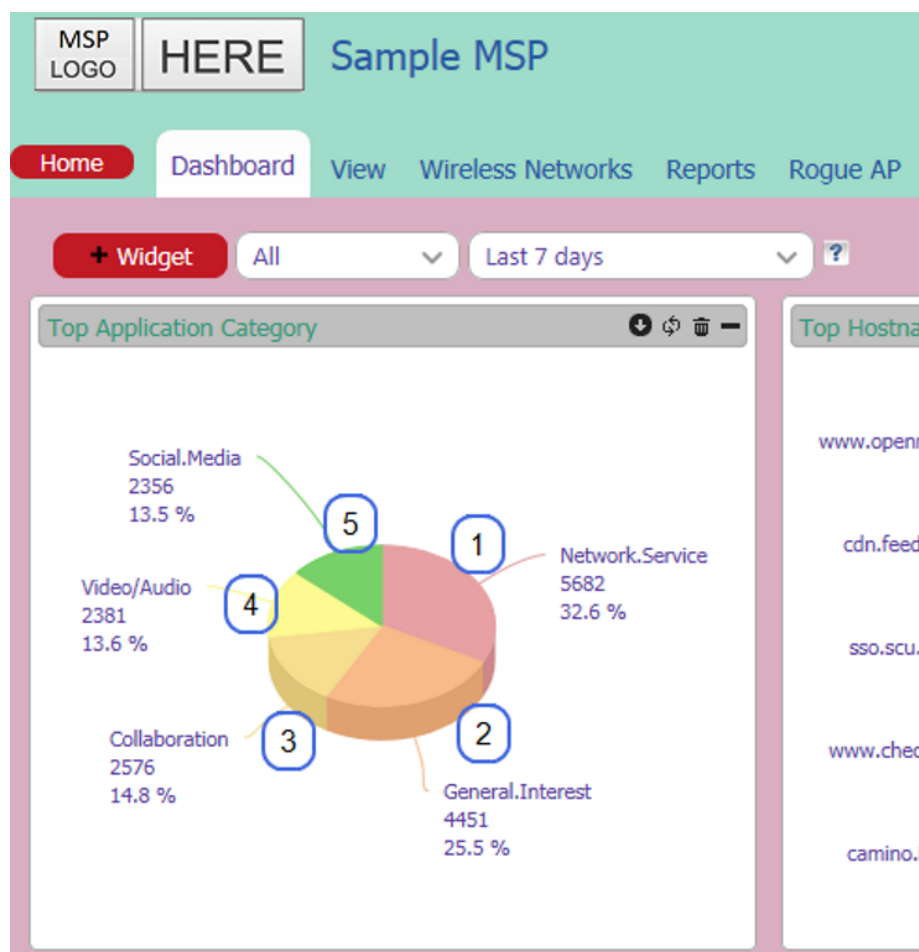


The following table describes the callout labels in the preceding figure:

Callout	Label	Description
1	Page	Background and text color for the overall page, excluding the header and footer
2	Page Header	Background and text color for the top portion of the page, including the tabs
3	Page Footer	Background and text color for the bottom portion of the page
4	Button	Background and text color for the buttons on the page
5	Widget header	Background and text color for the widgets on the dashboard, and for tables on the other pages

Chart Series Color Settings

Chart Series Color Settings refer to pie charts and bar charts on the dashboard page (see the table below for descriptions of the callout labels):

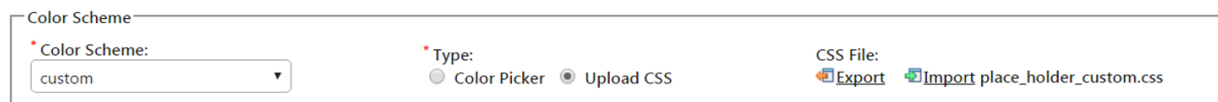


The following table describes the callout labels in the preceding figure:

Settings	Callout	Impacted Chart Segment
Series #1	1	First
Series #2	2	Second
Series #3	3	Third
Series #4	4	Fourth
Series #5	5	Fifth
Series #6		Sixth

Using a custom CSS file

Select *custom* in the Color Scheme selector and select *Upload CSS*.



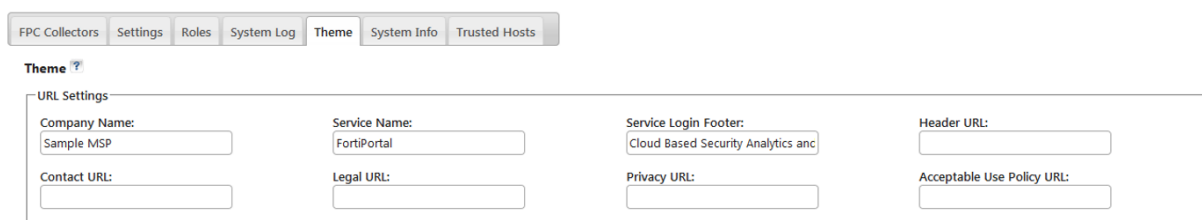
To update the CSS file, follow these steps:

1. Select *Export* to export the current CSS file. The file is saved in the Downloads folder of your local machine.
2. Edit the file to make changes as desired and save the file.
3. Select *Import*.
4. Use the file chooser to select your updated CSS file.

If the imported file contains any invalid CSS style, the style will be reset to the default CSS style.

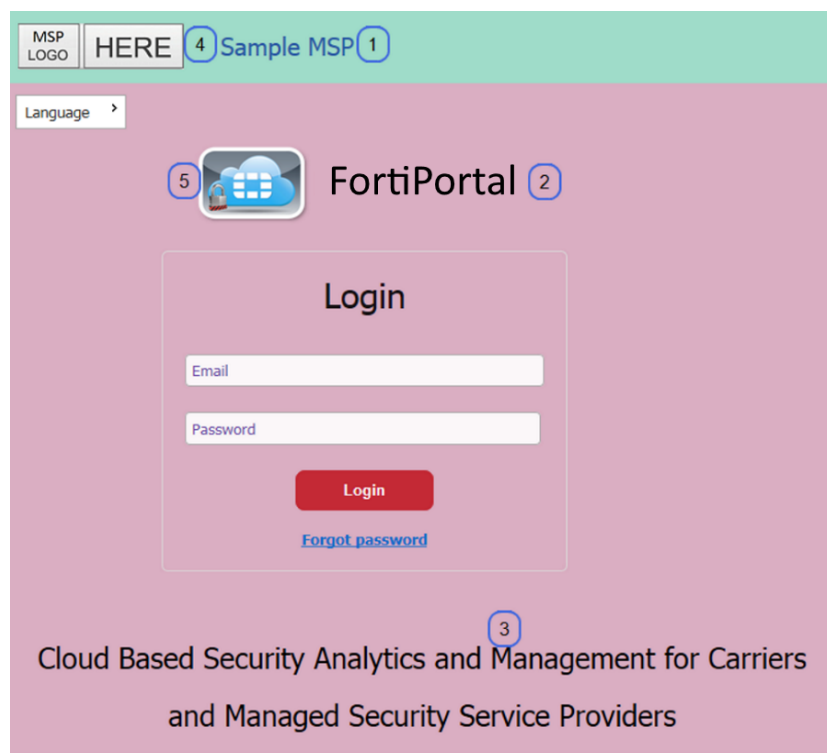
Custom URLs and text

The following figure displays the URL Settings panel.



The URL Settings panel sets URL and text fields for the login page. The maximum length of each custom text field is 100 characters.

The locations of the fields are shown in the following figure (see the table below for descriptions of the callout labels):



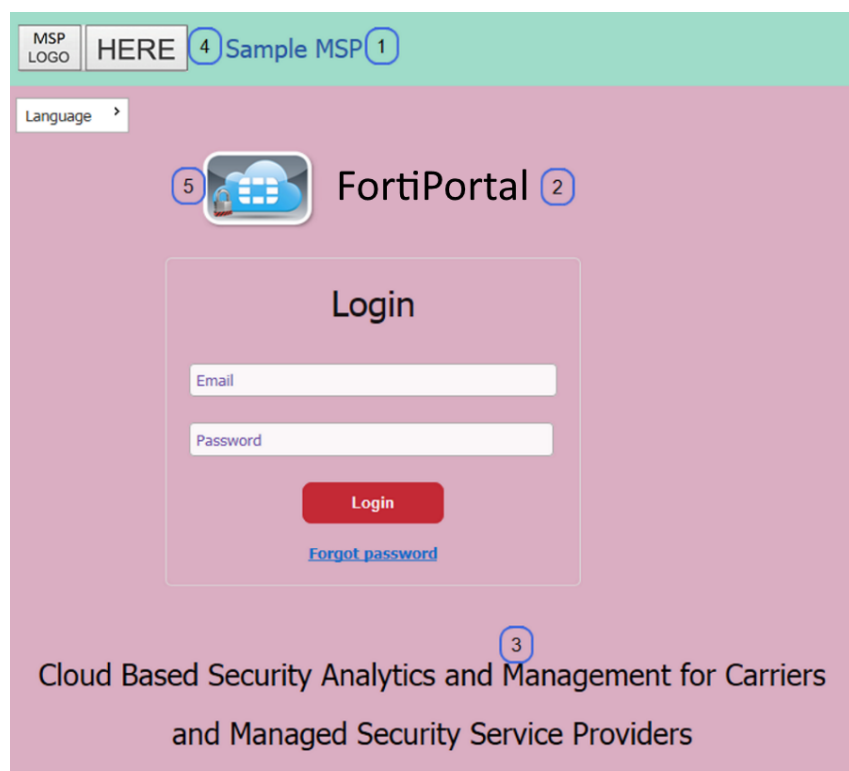
The following table describes the callout labels in the preceding figure:

Settings	Callout	What does it Display?
Company Name	1	Company name and header logo on the header of every page
Service Name	2	Service name and service logo image at the top of the login page
Service Login Footer	3	Service login footer at the bottom of the login page. (NOTE: The login page does not include a separate footer color.)

Custom images

The following figure shows the Images panel:

Some of the custom image fields refer to the login page. The locations of the fields are shown in the following figure (see the table below for descriptions of the callout labels):



The following table describes the callout labels in the preceding figure:

Settings	Callout	Description
Header Logo Image	4	
Service Logo Image	5	

Resizing images

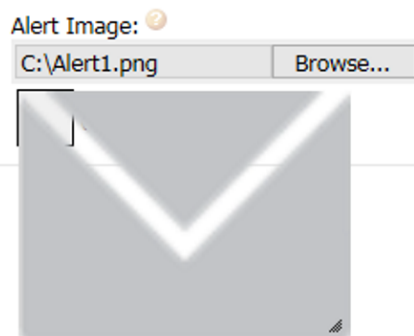
When you upload an image for one of the custom fields, the system displays a thumbnail of the image. If the uploaded image is too large, you can drag from the right edge and bottom edge of the image to resize it. You can also drag from the bottom right corner (or depress the shift key), to retain the current proportions of the image as it changes size.

For assistance in resizing the image, the system provides a sizing box, and also provides the image height and width.

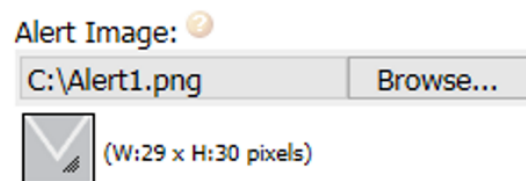
The help (?) icon for each image field provides the minimum and maximum dimensions for each image.

The following figure shows a downloaded alert icon image before resizing and after resizing:

Before resizing



After resizing




Details of the theme configuration fields

The following table describes the configuration fields:

Settings	Guidelines	Default value
Color Scheme	Select a color scheme for the Admin pages. Select the <i>Color Picker</i> icon to add (that is, edit) a custom color scheme.	Blue
Type	Visible for a custom scheme. Select <i>Color Picker</i> or <i>Upload CSS</i> .	Color Picker

Settings	Guidelines	Default value
Color Picker	Visible only when you select Color Picker as the color scheme type. Opens the Edit Custom Color Scheme form. See the "Using Color Picker" section for details.	n/a
CSS File	Visible when you select Upload CSS as the color scheme type. Displays buttons to export or import a CSS file.	n/a
Export	Exports the current CSS file. The file is saved in the Downloads folder of your local machine.	n/a
Import	Imports a file that replaces the current CSS file in use. Opens a file-chooser dialog allowing you to select a CSS file.	n/a
URL values for Header and Footer		
There are links in the header and footer to various corporate web pages. The following URL values must be public web pages. Specify the full URL, including "http://".		
Company Name	(mandatory field) Service Provider company name is displayed in the footer of each page.	n/a
Service Name	Service name to display on the login page	
Service Login Footer	Footer text to display on the login page	
Header URL	Link activated from the company logo in the header, and the company name in the footer. Specify the URL to open, such as your company home page.	blank
Contact URL	Footer contains a link to the Contact page. Specify the target URL.	blank
Legal URL	Footer contains a link to the Legal page. Specify the target URL.	blank
Privacy URL	Footer contains a link to the Privacy page. Specify the target URL.	blank
Acceptable Use Policy URL	Footer contains a link to the Acceptable Use Policy page	blank
Image files		
Unless otherwise stated, the supported file types for images include jpg, png, and gif.		

Settings	Guidelines	Default value
Favicon Image	(Uploaded) Image file that FortiPortal will use as a Favorites icon. Supported file types include ico, jpg, png, and gif. The recommended file type is .ico and the maximum image size is 20x20 pixels.	blank
Header Logo Image	Image file that FortiPortal will use for the header logo. The recommended image size is 144x48 pixels.	blank
PDF Logo Image	Image file that FortiPortal will use as the logo in PDF reports. The recommended image size is 144x48 pixels.	blank
Service Logo Image	Image file that FortiPortal will use as the logo on the login page. The recommended image size is 104x80 pixels.	
Icons in the page banner		
1. Alert Image	Image file for the alert icon in the page banner. The recommended image size is 30x30 pixels.	
2. Customer Count Image	Image file for the customer icon in the page banner. The recommended image size is 30x30 pixels.	
3. Users Image	Image file for the MSSP users icon in the page banner. The recommended image size is 30x30 pixels.	
4. Change Password Image	Image file for the change password icon in the page banner. The recommended image size is 30x30 pixels.	

System Info

Go to *Admin > System Info* to see additional information about the system.

System Info page

The page displays the following panels:

- License Information
- Version Information
- FPC Admin Login
- Certificate Information

License Information

This panel provides information about the FortiPortal license and enables you to upload a new license.

Field	Description
VM License	Indicates the type of license and whether the license is valid
Devices Allowed [Used]	Number of devices to be managed that are included in the license (number in brackets indicates the number of devices currently used)
FAPs Allowed [Used]	Number of Fortinet AP devices that are included in the license (number in brackets indicates the number of devices currently used)
FSA Devices Used	Number of Fortinet Sandbox devices that are in use
Expiry Date	Expiry date of the license
Serial Number	Your FortiPortal serial number.

Upload a license

You only need a single license file for FortiPortal. After you upload the FortiPortal license, the license details are shown in the *Admin > System Info* page, including the number of devices allowed, the number of devices used, the number of Fortinet Access Points (FAPs) allowed, the number of FAPs used, and the number of FortiSandbox (FSA) devices used.

The number of devices used is the number of devices (VDOMs) that a Managed Security Service Provider (MSSP) user assigns to a customer site. Other devices that FortiPortal has access to from FortiManager do not count as “used” until they are assigned to a customer site.

If the MSSP user creates a customer site, assigns a device to it, and the MSSP user has selected the FortiSandbox checkbox so that FortiPortal will process logs from the customer’s FortiSandbox devices, those devices are counted as part of the number of devices used. Refer to the *Admin > System Info* page.

When the MSSP user removes a device from the customer site, the number of devices used decreases by one, and the number of devices allowed increases by one. Refer to the *Admin > System Info* page.

The Expiry Date on the *Admin > System Info* page shows when the FortiPortal license expires.

Use the following steps to upload the FortiPortal license:

1. Go to *Admin > System Info* and locate the License Information panel.
2. Under the *Upload License* label, select *Browse*.
The system opens a file chooser window.
3. Select a license file and select *Open*.
4. The system automatically restarts the FortiPortal VM to apply the license.

The screenshot shows the FortiPortal Admin interface. The top navigation bar includes Home, Dashboard, Customers, Devices, Admin (selected), and Audit. A status bar on the right indicates 0.08 MB used of 100.00 GB. Below the navigation bar, there are tabs for Settings, Roles, System Log, Theme, System Info (selected), Trusted Hosts, and Additional Resources. The main content area is titled 'System Info' and contains four panels:

- License Information:** A table showing license details.

VM License	Valid ✔
Devices Allowed[Used]	10 [3]
FAPs Allowed[Used]	100 [0]
FSA Devices Used	0
Expiry Date	Fri Jun 08 00:16:44 2018 GMT
Serial Number	FPC-VM1000000008

 Below the table is an 'Upload License' section with a 'Choose File' button (No file chosen), 'Save', and 'Cancel' buttons.
- Version Information:** A table showing version details.

Version	5.0.0
Build Number	7
- FPC Admin Login:** A section with an 'FPC Admin >' button.
- Certificate Information:** A section with 'Certificate' and 'Private Key' fields, each with a 'Choose File' button (No file chosen), and 'Save' and 'Cancel' buttons.

Version Information

The Version Information panel displays the FortiPortal version and the build number.

FPC Admin Login

The FPC Admin Login panel contains a link to allow you to log in as an administrator.

Certificate Information

The Certificate Information panel displays the certificate file name and private key file name.

From this panel, you can select and upload a new certificate and private key for the FortiPortal (using PKCS#8 format).

Trusted Hosts

If you enable Trusted Hosts as a global setting (see "[Admin settings](#)" on page 72), the system enforces a configurable blacklist and whitelist for all admin and customer users. The Trusted Hosts displays the blacklist. Refer to "[Administrative users](#)" on page 31 for information about creating the Trusted Hosts whitelist.

Go to *Admin > Trusted Hosts* to see the IP Blacklist where you can create and edit blacklist entries.

The screenshot shows the 'Trusted Hosts' page in a web interface. At the top, there's a navigation bar with tabs: 'FPC Collectors', 'Settings', 'Roles', 'System Log', 'Theme', 'System Info', and 'Trusted Hosts'. Below this, the 'Blacklist' section is active. It features a '+ Add' button on the right. On the left, there's a 'Show 10 entries' dropdown menu. To the right of this is a search bar labeled 'Search' with the placeholder text 'Search by Name'. Below these elements is a table with four columns: 'IP Start', 'Mask', 'Prefix', and 'Action'. The table is currently empty, and the text 'No data available' is centered at the bottom of the table area.

Page actions

The Roles page contains the following actions:

- **+ Add**—open a new page with the form to add a blacklist entry
- **Search**—enter text to search for roles containing that text

Per-role actions

When you scroll over a entry in the roles list, the following icons appear in the Action column:

- **Edit**—opens a new page with the form to edit a Trusted Host
- **Delete**—deletes the Trusted Host

The following figure shows the Add Trusted Host form:

Add Trusted Host

*

IP Start:

*

Mask:

*

Prefix:

-1

Save

Cancel

The Add/Edit Trusted Host forms contain the following fields:

Settings	Guidelines
IPv4	
IP Start	Start address for the range covered by this entry
Mask	Defines the range of IP addresses covered by this entry
IPv6	
IP Start	Start address for the range covered by this entry
Prefix	Defines the range of IP addresses covered by this entry



Additional Resources

Go to *Admin > Additional Resources* to see the button (resource) list, which enables administrators to add, edit, delete, or view the displayed resources:

FPC Collectors	Settings	Roles	System Log	Theme	System Info	Trusted Hosts	Additional Resources
----------------	----------	-------	------------	-------	-------------	---------------	----------------------

Button List ?
+ Add

Show 10 entries
 Search

Name	URL	Image	Status	Action
Help	www.serviceprovider.com/help	ContactUs.jpg	✓	
chat	www.serviceprovider.com/chat	Feedback.jpg	✓	 
FAQ	www.serviceprovider.com/faq	FAQ.jpg	✓	

Page actions

The Button List page contains the following actions:

- **+ Add**—open a new page to add a resource
- **Search**—enter text to search for resources containing that text

Selecting **+ Add** opens the Add Button window:


FPC Collectors
 Settings
 Roles
 System Log
 Theme
 System Info
 Trusted Hosts
 Additional Resources

Button List ?
+ Add

Show 10 entries
 Search

Name	URL	Image
Help	www.serviceprovider.com/help	ContactUs.jpg
chat	www.serviceprovider.com/chat	Feedback.jpg
FAQ	www.serviceprovider.com/faq	FAQ.jpg

Add Button
 ✕

* Name:
 * URL:
 * Status: ☒ Active ☐ Disabled
 Image: Browse...
 (W:72 x H:72 pixels)
Save Cancel

Enter the following button details:

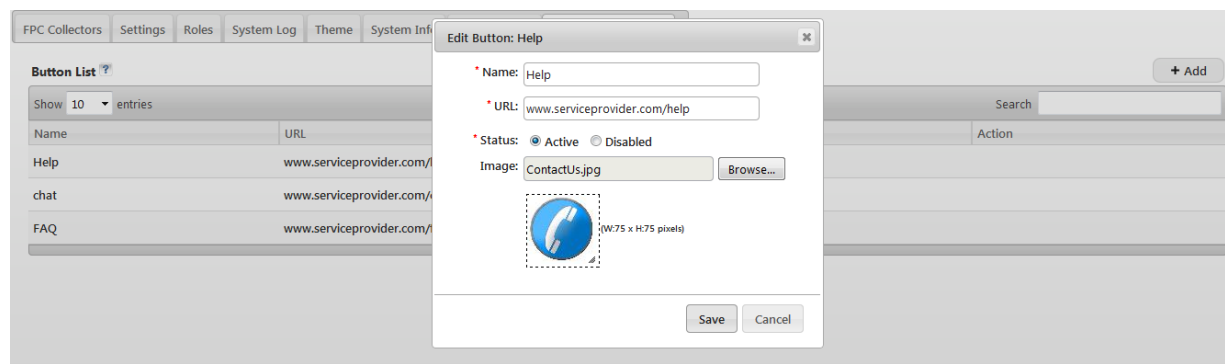
Field	Description
Name	Button or resource name
URL	Link to open when the button is selected
Status	Active or Disabled
Image	Default image is pre-populated. You can change or resize it with the <i>Browse</i> button and resize icon.

Per-role actions

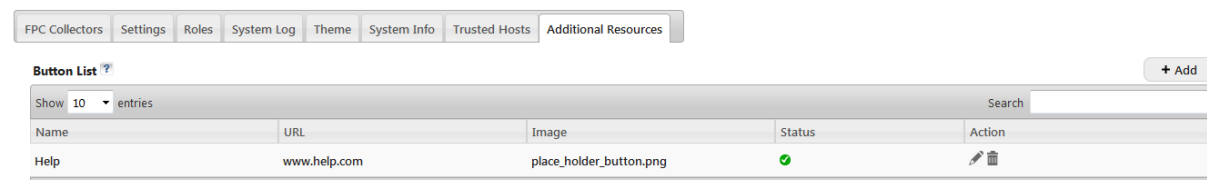
When you hover over a button row, the following icons appear in the Action column:

- *Edit*—opens a new page with the form to edit an existing role
- *Delete*—deletes the selected role

Selecting *Edit* displays the Edit Button: *button* form, where *button* can be Chat, FAQ, or Help:




At any time, you can select the *Delete* icon to remove the button row:



Audit

The Audit tab displays an log of user activity on the Administrative Web Interface:

Audit Log List Last 1 Day 

[Export to CSV](#)

Show 10 entries					Search <small>Search by Level/User Name/Event Type/Client IP Address/Message</small>
Date	Level	User Name	Event Type	Client IP Address	Message
2016-01-25 10:49:36	info	spuser	Add Site	172.30.12.40	Site: Site2 was added and assign to customer: Customer2
2016-01-25 10:49:22	info		Login	172.30.12.44	Login: User (spuser) was logged in
2016-01-25 10:49:17	info	spuser	Add Customer	172.30.12.40	Customer: Customer2 was added
2016-01-25 10:48:45	info	spuser	Add Wifi	172.30.12.40	Wifi: Wifi1 was added and assign to customer: Customer1
2016-01-25 10:48:34	info	spuser	Add Site	172.30.12.40	Site: Site1 was added and assign to customer: Customer1
2016-01-25 10:48:12	info	spuser	Add Customer	172.30.12.40	Customer: Customer1 was added
2016-01-25 10:47:48	info	spuser	Add Controller	172.30.12.40	Controller: root/Controller/vd12 was added
2016-01-25 10:47:15	info	spuser	Add Forti Manager	172.30.12.40	Forti Manager: FM was added
2016-01-25 10:46:55	info	spuser	Add Collector	172.30.12.40	Collector: Collector2(172.30.71.134) was added
2016-01-25 10:46:24	info	spuser	Add Collector	172.30.12.40	Collector: Collector1(172.30.71.245) was added

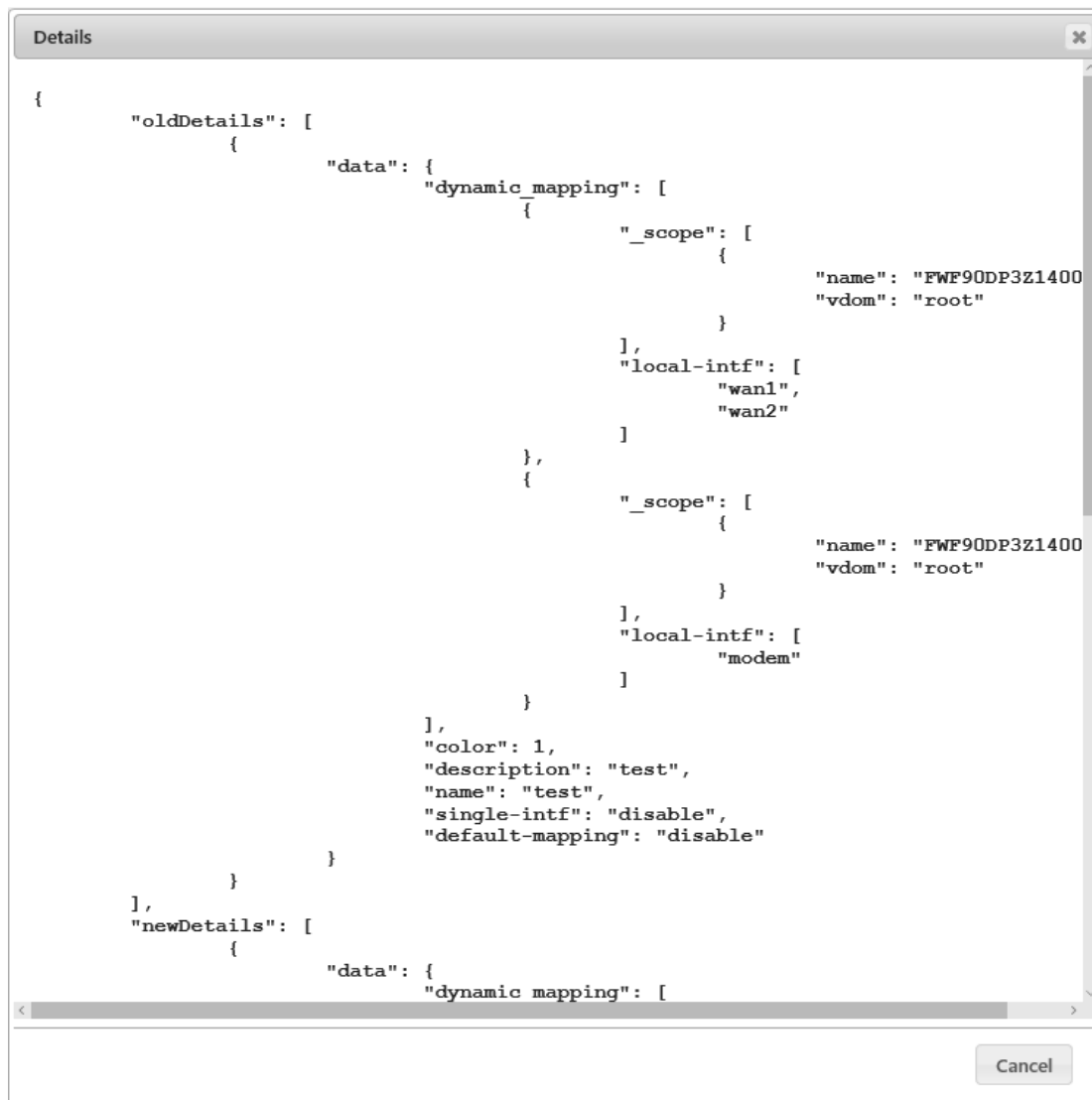
Showing 1 to 10 of 14 entries First Previous 1 2 Next Last

Page actions

- **Audit Log List**—set the duration of the logs to display (last 60 minutes, last 1 day, last 7 days, or customize)
- **Search**—use any column to search the audit log list by level, user name, event type, client IP address, or message
- **Export to CSV**—export the audit log list as a Comma-Separated Value (CSV) file

Per-audit actions

When you select the *Message* field for an *Edit Customer* audit entry, the system opens a pop-up window to display the details of the change. The details window shows the original ("oldDetails") and new ("newDetails") field values:



Upgrading FortiPortal software

This section provides instructions to upgrade FortiPortal from an earlier version to a more recent version.

NOTE: For FortiPortal 5.0 and later, you must download a new license file from <https://support.fortinet.com/>.

To upgrade from version 4.2.0 or later, you can upgrade directly to version 5.0.0.

To upgrade from version 3.2.2 or earlier, you must:

1. Perform a sequential set of upgrades to version 4.0.0.
2. Upgrade from version 4.0.0 to version 4.1.2.

If you are upgrading from a version prior to version 4.0.0, refer to [Table 1](#) on page 116 to determine your upgrade path. Find your existing version in the *Existing Version* column of the table and determine the more recent version(s) to which you can upgrade in the *Compatible Upgrade Version* column. When you upgrade to a more recent version, repeat this process until you're running the most recent version.

Table 1: Upgrade Path

Existing Version	Compatible Upgrade Version
2.1.0	2.1.1
2.1.1	2.2.0
2.2.0	2.2.1, 2.2.2, 2.3.0
2.2.1	2.2.2, 2.3.0
2.2.2	2.3.0
2.3.0	2.3.1
2.3.1	2.4.0, 2.4.1
2.4.0	2.4.1, 2.5.0, 3.0.0
2.4.1	2.5.0, 2.5.1, 3.0.0, 3.1.0
2.5.0	2.5.1, 3.0.0, 3.1.0
2.5.1	3.0.0, 3.1.0, 3.1.1, 3.1.2
3.0.0	3.1.0, 3.1.1, 3.1.2
3.1.0	3.1.1, 3.1.2, 3.2.0
3.1.1	3.1.2, 3.2.0

Existing Version	Compatible Upgrade Version
3.1.2	3.2.0, 3.2.1, 3.2.2
3.2.0	3.2.1, 3.2.2, 4.0.0
3.2.1	3.2.2, 4.0.0, 4.0.1
3.2.2	4.0.0, 4.0.1, 4.0.2, 4.0.3
4.0.0	4.1.2
4.0.1	4.1.2
4.0.2	4.1.2
4.0.3	4.1.2
4.0.4	4.1.2
4.1.0	4.2.0, 4.2.1, 4.2.2, 4.2.3
4.1.1	4.2.0, 4.2.1, 4.2.2, 4.2.3
4.1.2	4.2.0, 4.2.1, 4.2.2, 4.2.3
4.2.0	4.2.1, 4.2.2, 4.2.3, 5.0.0
4.2.1	5.0.0
4.2.2	5.0.0
4.2.3	5.0.0

Upgrade procedures

Complete the following tasks to perform an upgrade:

1. From the Fortinet Customer Service & Support website (<https://support.fortinet.com/>), download the portal and/or collector build files for VMware (the `.out` files, not the `.ovf.zip` files) for the version to which you want to upgrade.
2. Perform a backup of the portal and collector MySQL database(s). For details, see "Perform a backup" on page 118.
3. To prevent the collectors from processing logs during the upgrade, shut down the collectors from the VM console.
4. *Restart the portal.* From the VM console, log in as admin and type `execute reboot`.
5. Upgrade the portal. For details, see "Upgrade the portal" on page 118.

6. Turn on the collector(s). For example, from the vSphere client, right-click the collector(s) and go to *Power > Power On*.
7. Upgrade the collector(s). For details, see "[Upgrade the collector](#)" on page 119



Do *not* turn off or restart the portal or collector(s) while upgrading. Doing so can cause a loss of data and otherwise harm the system.

Perform a backup

NOTE: You can use <https://mysqlbackupftp.com> to back up the portal and collector database.

1. You can export (or create a snapshot of) a VM for a backup. For example, for VMware, from the vSphere client, shut down the database VMs from the VM console. If you are using the sample MySQL database, log in as user `fpc`, get root privileges, type `sudo su`, and type `shutdown now`.
2. For VMware users, go to *File > Export > Export OVF Template* to export the VM.
3. For *Name*, set a name for the backup.
4. For *Directory*, select a directory from which you can restore the backup to vSphere.
5. Optionally, enter a *Description* for the backup.
6. Select *OK*.
7. After the backup is complete, right-click the virtual machine you backed up and go to *Power > Power On*.

Upgrade the portal

1. Log in to the portal using a service provider (administrator) account.
2. Select the *Admin* tab.
3. Select *FPC Admin* to open the administrator portal. The administrator portal opens in a new browser tab.
4. Log in to the administrator portal. The default user name is `admin`, and there is no default password.
5. Select the *System Settings* tab.
6. In the *System Information* widget, select the *Update* button beside the *Firmware Version*.
7. In the pop-up dialog, select *Choose File* and select the portal `.out` file that you downloaded in Step 1 in "[Upgrade procedures](#)" on page 117.
8. Select *OK*. The portal will upgrade. After the firmware is upgraded, the system will restart automatically.



Check that the version number in the *Admin > System Info > Version Information > Version* field in the FortiPortal administrative web interface matches the version number in the administrator portal (*System Settings > Dashboard > Firmware Version*). If these two numbers do not match, the portal has not finished upgrading. You must wait for the portal to finish upgrading before upgrading the collector.

NOTE: If you have a RADIUS server configured in an existing version, you must re-enter the RADIUS attributes after the portal upgrade is complete. For details, see the *FortiPortal Administration and User Guide*.

Upgrade the collector

For a collector HA cluster, first upgrade the master and then the slave(s). Repeat these steps for each collector:

1. Restart each collector, one at a time.
2. Log in to the portal using a service provider (administrator) account.
3. Select the *Devices* tab.
4. Select the *FPC Collectors* tab.
5. Click the IP address of the collector to open that collector's administrator portal. The administrator portal opens in a new browser tab.
6. Log in to the administrator portal. The default user name is `admin`, and there is no default password.
7. Go to *System Settings*.
8. In the *System Information* widget, select the *Update* button beside the *Firmware Version*.
9. In the pop-up dialog, select *Choose File* and select the collector `.out` file that you downloaded in Step 1 in ["Upgrade procedures"](#) on page 117.
10. Select *OK*. The collector will upgrade. After the firmware is upgraded, the system will restart automatically.

Alert messages

FortiPortal generates the following alert messages. The Service Provider level messages include the name of the customer (XXXX in the list below).

Service-provider level messages:

Total Storage reached 90 % for customer(XXXX)

Collector Storage reached 90 % for customer(XXXX)

FPC Storage reached 90 % for customer(XXXX)

Email server credentials are invalid

Failed to send the report

Please make sure all device assign to customer(XXXX) on same collector.

Wifi: Unassigned FAP(s): (XXXX)

Cannot connect to the database: URL Name

Delete data process for Customer(XXXX) Started

Delete data process for Customer(XXXX) ended

Delete data process for Site(XXXX) Started

Delete data process for Site(XXXX) ended

Delete data process for unassigned device(XXXX) Started

Delete data process for unassigned device(XXXX) ended

Delete data process for wifi network(XXXX) Started

Delete data process for wifi network(XXXX) ended

Unable to connect <Fpc Database> : XXXX

Unable to connect <Collector Database>: XXXXX

Unable to connect <Collector>: XXXX

Unable to connect <FortiManager> : XXXX

Failed to poll Fortimanager: XXXX

Wrong remote user authentication settings : XXXX

Collector cleanup alert messages : XXXX

Cleanup for collector storage : customer <Customer Id>

Settings are successfully saved. For authentication related changes please reboot system.

Customer-level messages:

Total Storage reached 90 %, contact your service provider

Storage reached 90 %, contact your service provider

FPC Storage reached 90 %, contact your service provider

Appendix: Sizing

Before you start your setup, you need to determine the storage requirements for the portal and collector databases. To do this, determine the approximate values for the following:

- Expected log rate (logs per second)
- Number of customers
- Number of days to retain data
- Number of FortiGate devices

NOTE: The values are based on one VDOM per customer and an 80/20 storage ratio of the portal database to the collector database. If you are using FortiGate HA, count only the number of HA masters for the number of FortiGate devices.

The expected log rate is the *overall value* for logs to the collector. To find the number of logs per second for a VDOM based on the last seven days of logs, use the `diagnose test application` command.

For example:

```
FG1K5D3I14801425 # diagnose test application miglogd 4
info for vdom: root
memory
traffic: logs=63016358 len=34499571723, Sun=0 Mon=0 Tue=63016358 Wed=0 Thu=0 Fri=0
Sat=0
event: logs=2756 len=972616, Sun=324 Mon=324 Tue=345 Wed=324 Thu=740 Fri=375 Sat=
t=324
```

The example shows the log counters for a seven-day period and gives the total number of entries for each log type for each VDOM.

To calculate the number of log entries per second, take the sum of the logs (for example, 63,016,358 + 2,756 = 63,019,114), divide by 7 (for example, 63,019,114/7 = 9,002,731), and then divide by 86,400 (for example, 9,002,731/86,400 = 104) to get the number of logs per second.

A single collector instance (collector and database) can handle 15,000 logs per second. The portal supports multiple collectors on multiple VDOMs to increase the log rate and storage.

The following calculations can be used to determine the storage values for the collector and the portal and collector databases:

$\text{Syslog /second /customer} = \text{expected log rate} / \text{number of customers}$

$\text{Portal database size in MB for one syslog /second /day size} = 0.156$

$\text{Portal database size in GB /customer /day} = (\text{syslog /second /customer} * 0.156) / 1024$

$\text{Portal database size /customer to retain data} = \text{portal database size in GB /customer /day} * \text{number of retention days}$

$\text{Minimum customer storage} = \text{portal database size /customer to retain data} / (0.8 * 0.2)$ (The minimum value is 5 GB.)

$\text{Collector disk size} = 2.65 + (\text{number of FortiGate units} * 3.25)$ (The minimum value is 80 GB.)

$\text{Portal database disk size} = \text{minimum customer storage} * \text{number of customers} * 1.25 * 0.2 + 20$

Collector database disk size = minimum customer storage * number of customers * **1.25** * 0.8 + **20**

NOTE: Values in boldface are either buffer values or allocations for system files.

For example:

Expected log rate	500
Number of customers	5
Number of retention days	60
Number of FortiGate units	10

When you substitute these values into the calculations:

Syslog /second /customer = $500 / 5 = 100$

Portal database size in GB /customer /day = $(100 * 0.156) / 1024 = 0.015$

Portal database size /customer to retain data = $0.015 * 60 = 0.914$

Minimum customer storage = $0.914 / (0.8 * 0.2) = 5.712 \sim 6$ GB

Collector disk size = $2.65 + (10 * 3.25) = 35.15$ GB, so use the minimum value of 80 GB

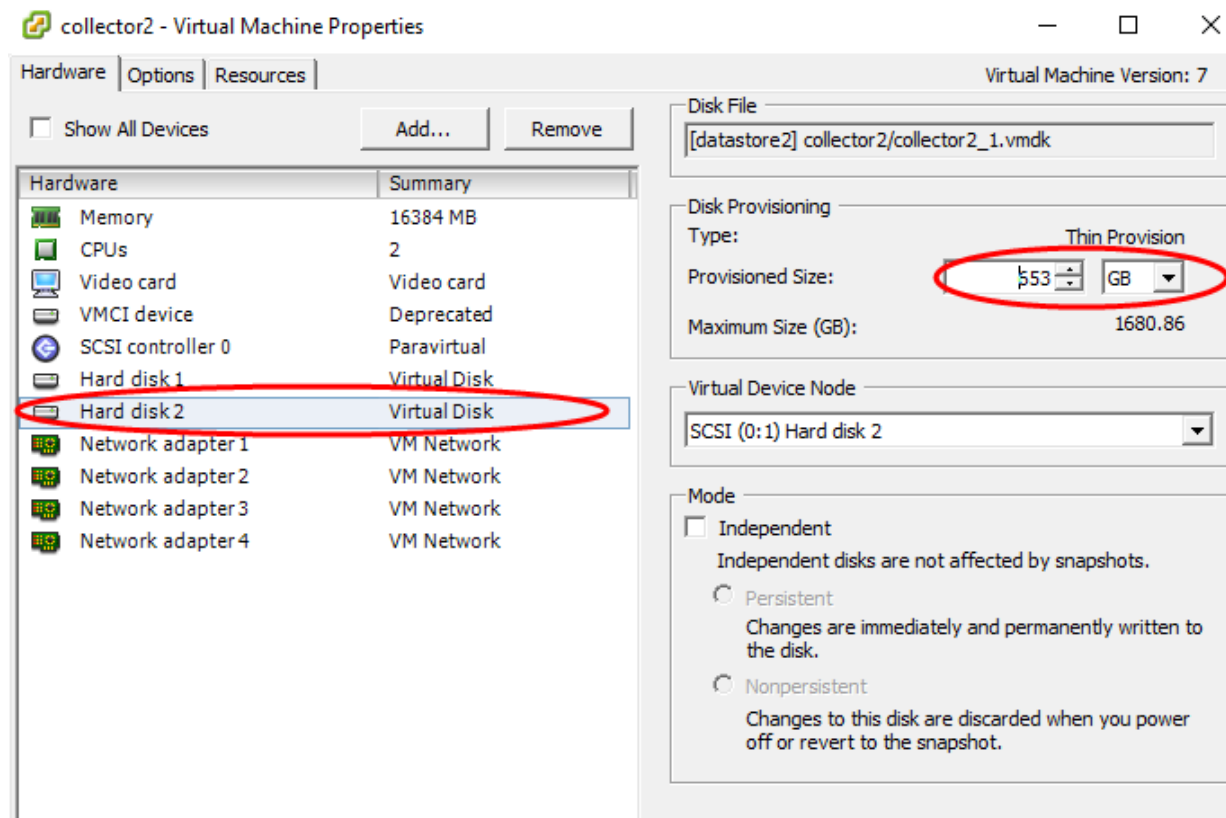
Portal database disk size = $6 * 5 * 1.25 * 0.2 + 20 = 27.5$ GB

Collector database disk size = $6 * 5 * 1.25 * 0.8 + 20 = 50$ GB

Configuring the collector VM disk size

NOTE: The NTP source must be the same for all portal and collector VMs to synchronize the log time stamps across all devices.

When you deploy the OVF image for the first time, you can configure the disk size. There are two virtual disks. Hard disk 1 is the flash disk (2 GB); hard disk 2 is the storage disk (80 GB by default.). You can increase the size of the storage disk when deploying the VM. See the following figure. (Do not increase the size of hard disk 1.)



When the collector is running, use the `execute lvm info` command to see the disk size.

```
FPCVM64 # execute lvm
  extend  Extend LVM logical volume.
  info    Get system LVM information.
  start   Start using LVM.

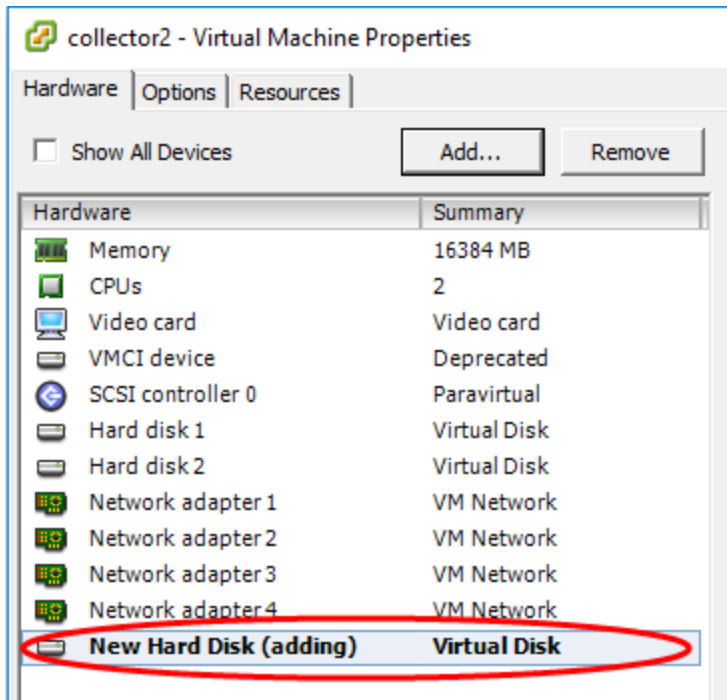
FPCVM64 # execute lvm info
Disk1 :      Used      684GB
Disk2 : Unavailable    0GB
Disk3 : Unavailable    0GB
Disk4 : Unavailable    0GB
Disk5 : Unavailable    0GB
Disk6 : Unavailable    0GB
Disk7 : Unavailable    0GB
Disk8 : Unavailable    0GB
Disk9 : Unavailable    0GB
Disk10 : Unavailable   0GB
Disk11 : Unavailable   0GB
Disk12 : Unavailable   0GB

FPCVM64 #
```

If you have already deployed the collector VM, you can add an additional disk.

To add a disk:

1. Shut down the collector.
2. Edit the VM properties.
3. Add an additional disk. See the following figure.



4. Start the collector.
5. Use the `lvm info` command again. You should now see an additional, unused disk.

6. Enter the `execute lvm extend` command to use the new hard disk. The collector will reboot.

```
FPCVM64 # execute lvm extend
LVM   Disk(s) [Disk1 Disk2 ...]

Disk1 :      Used      684GB
Disk2 :      Unused    104GB
Disk3 : Unavailable    0GB
Disk4 : Unavailable    0GB
Disk5 : Unavailable    0GB
Disk6 : Unavailable    0GB
Disk7 : Unavailable    0GB
Disk8 : Unavailable    0GB
Disk9 : Unavailable    0GB
Disk10: Unavailable    0GB
Disk11: Unavailable    0GB
Disk12: Unavailable    0GB

FPCVM64 # execute lvm extend
Disk2 will be added to LVM.
This operation will need to reboot the system.
Do you want to continue? (y/n)
```

7. When the collector is running, use the `execute lvm info` command to see the new disk size.

```
FPCVM64 #
FPCVM64 # execute lvm info
Disk1 :      Used      684GB
Disk2 :      Used      104GB
Disk3 : Unavailable    0GB
Disk4 : Unavailable    0GB
Disk5 : Unavailable    0GB
Disk6 : Unavailable    0GB
Disk7 : Unavailable    0GB
Disk8 : Unavailable    0GB
Disk9 : Unavailable    0GB
Disk10: Unavailable    0GB
Disk11: Unavailable    0GB
Disk12: Unavailable    0GB

FPCVM64 #
```

Appendix: Installation using OpenStack

The FortiPortal software runs on virtual machines. Each VM runs either the portal or the collector software.

You can use OpenStack to create and manage the VM instances.

Prerequisites

Note the following prerequisite items:

1. You must provide a MySQL server for the portal database, and one or more MySQL servers for the collector database instances.
2. Download the portal and collector images from Fortinet Support site.
3. Access to OpenStack Horizon Dashboard for your OpenStack environment.

Downloading FortiPortal image files

To download the required image files.

1. Navigate to the Fortinet customer service page (<https://support.fortinet.com>).
2. Go to *Download > Firmware Images*.
3. In Firmware Images page, select *FortiPortal*.
4. Download the latest image files (one portal file and one collector file) in QCOW2 format:
 - fpcvm64imageCollector.out.qcow2
 - fpcvm64imagePortal.out.qcow2

OpenStack Horizon Dashboard

Log in to the OpenStack Horizon Dashboard, which provides a web-based user interface to OpenStack services.

Create images for the portal and collectors

Create a portal image and a collector image.

Use the following steps to create an image:

1. From the left menu, select *Compute > Images*.
2. Select *Create Image*.
3. System opens a form. Enter the following fields in the form:
 - a. Enter a unique name for the image.
 - b. Image Source: select *Image File*.

- c. Select *Choose File* to open the file chooser.
- d. Select the portal or collector file that you saved on the hard drive.
- e. Format: QCOW2.
- f. Architecture: leave blank.
- g. Minimum Disk: 80.
- h. Minimum Ram: 16.
- i. Select *Create Image*.

Create volumes for the portal and collector

Create a storage volume for the portal and the collector.

Use the following steps to create a volume:

1. Select *Volumes* in the main menu.
2. Select *Create Volume*.
3. System opens a form. Enter the following fields in the form:
 - a. Enter a unique name for the volume.
 - b. *Volume Source*: No source, empty volume.
 - c. *Type*: No volume type.
 - d. *Size*: 80.
 - e. *Availability Zone*: select a zone.
 - f. Select *Create Volume*.

Launch the instances

Launch one instance for the portal and one for the collector.

To launch a VM instance:

1. Select *Instances* in the main menu.
2. Select *Launch Instance*.
3. System opens a form. Enter the following fields in the Details tab of the form:
 - a. *Availability Zone*: select a zone.
 - b. *Instance Name* Enter a unique name for the instance.
 - c. *Flavor*: Select the appropriate size of VM.
 - d. *Instance Count*: You can create one or more instances.
 - e. *Instance Boot Source*: Select Boot from image.
 - f. *Image Name*: Select the image name.
4. In the Access & Security tab:
 - a. *Key Pair*: Select a key pair.
 - b. *Security Groups*: Select the default.
5. In the Networking tab:
 - a. *Available networks*: Select a network.
6. Select *Launch*.

Launch one instance for the portal and one for the collector.

Assign a floating IP address

To associate an IP address to the instance:

1. Select *Instances* in the main menu.
2. In the Actions column, select *Associate Floating IP* in the pull-down list.
3. Select the + key to obtain an available IP address.
4. Select *Associate*.
Note the Floating IP address value. You will need this to configure the IP interface.

Associate the volume to the instances

To associate the storage volume to the instance:

1. Select *Volumes* in the main menu.
2. In the Actions column of the new volume, select *Manage Attachments* in the pull-down list.
3. Select the instance to associate.
4. Select *Attach Volume*.

Reboot the instances

To reboot the instance:

1. In the Action column, select *Hard Reboot* in the pull-down list.

Determine the IP address and port number

After the reboot, use the FortiPortal CLI to determine the IP address and external port number for each instance:

1. Select *Instances* in the main menu.
2. *Note the instance internal IP address.*
3. Select the instance name. The system displays the instance overview.
4. Select the *Console* tab.
5. Log in using default credentials.
6. Run the interface configuration command, and *note the Ethernet port number*:

```
exe shell
  ifconfig
exit
```

Configure the portal parameters

After the reboot, use the FortiPortal CLI to configure the portal parameters. Configure the parameters using the following steps:

1. Open the *OpenStack* console tab to view the console for the portal.
2. Log in using the default user ID (admin, with no password required).
3. Use the CLI instructions (see the steps below) to set the following parameters:

Setting	Description
Hostname	Host name for the portal VM
IP address and Default Gateway	Floating IP address for the portal VM and the route to the default gateway
SQL settings	Floating IP Address of the portal SQL server, database name, user credentials.
NTP settings	IP Address of the NTP server

NOTE: For the portal VM and SQL server, use the Floating IP addresses created in ["Assign a floating IP address "](#) on page 129.

CLI steps

1. Configure the host name for the portal VM:

```
config system global
    set hostname <host name>
end
```

2. Configure the system IP address and default gateway for the portal VM:

```
config system interface
    edit <port number>
        set ip <IP address> <mask>
        set allowaccess ping https http ssh snmp telnet
    end
config system route
    edit 1
        set device <port number>
        set gateway <default gateway>
    next
end
```

3. Configure the SQL settings:

```
config system sql
    set status remote
```

```

set database-type mysql
set database-name fp_fazlite
set username <portal database mySQL username>
set password <portal database mySQL password>
set server <IP address for the portal database>
end

```

4. Configure the NTP settings for the portal VM:

```

config system ntp
config ntpserver
edit 1
set server <NTP server>
end
set status enable
end

```

5. Reboot the VM.

Configure the collector parameters

After the reboot, use the FortiPortal CLI to configure the collector parameters. Configure the parameters using the following steps:

1. Open the *OpenStack* console tab to view the console for the collector.
2. Log in using the default user ID (admin, with no password required).
3. Use the CLI instructions (see the steps below) to set the following parameters:

Setting	Description
Hostname	Host name for the collector VM
IP address and Default Gateway	Floating IP address for the collector VM and the route to the default gateway
SQL settings	IP address of the portal SQL server, database name, user credentials.
NTP settings	IP address of the NTP server

NOTE: Always enter the database information for the portal database even when you are configuring a collector VM.

CLI steps

1. Configure the host name for the collector VM:

```

config system global
set hostname <host name>
end

```

2. Configure the system IP address and default gateway for the collector VM:

```
config system interface
  edit <port number>
    set ip <IP address> <mask>
    set allowaccess ping https http ssh snmp telnet
  end
config system route
  edit 1
    set device <port number>
    set gateway <default gateway>
  next
end
```

3. Configure the SQL settings:

```
config system sql
  set status remote
  set database-type mysql
  set database-name <database name>
  set username <portal database mySQL username>
  set password <portal database mySQL password>
  set server <IP address for the portal database>
end
```

4. Configure the NTP settings for the collector VM:

```
config system ntp
  config ntpserver
    edit 1
      set server <ntp server>
    end
  set status enable
end
```

5. Reboot the VM.

Updating the SSL certificate file

Use the following steps to import an SSL certificate for the FortiPortal VM.

From the Admin portal, select *Admin > System Info* to display information about the SSL certificate.

System Info page

The Certificate Information panel displays the certificate file name and private key file name.

From this panel, you can select and upload a new certificate and private key for the FortiPortal (using the PKCS#8 format).

Installing MySQL for FortiPortal databases

The MySQL database server for the portal or collector is a standard physical or virtual server.

Edit the my.cnf file to adapt the MySQL configuration for FortiPortal:

1. Edit the bind address to make the database reachable from the FortiPortal:
bind-address = <IP address of the database server>
2. Fortinet recommends that you create a dedicated MySQL user for FortiPortal. You will need to know the credentials for this user when you create the portal.

Notes:

- The portal database bind-address should match the SQL server address that you configure in the SQL settings of the portal (see *Configure Portal Parameters*).
- The collector database bind-address should match the SQL server address that you configure when you add a collector. See *FortiPortal Collectors*.
- If you are using MySQL 5.7.x, please add the following lines in the my.cnf file:
 - [mysqld] sql_mode = STRICT_TRANS_TABLES,NO_ZERO_IN_DATE,NO_ZERO_DATE,ERROR_FOR_DIVISION_BY_ZERO,NO_AUTO_CREATE_USER,NO_ENGINE_SUBSTITUTION

Reconfiguring MySQL password on FortiPortal

If you change the password for the FortiPortal user in the portal MySQL database, you need to update the configuration in the portal and collector:

```
config system sql
  set status remote
  set database-type mysql
  set password <portal db mySQL password>
end
```

Part II: User Guide

FortiPortal web interface

To analyze your event log data in the FortiPortal, customize reports, view the status of your network devices, view and configure security policies, you can use the FortiPortal web interface.

After a successful log in, the interface displays the dashboard page.

NOTE: To select a different language for this session, log out and select a language on the log-in page.

The top banner is common for all of the pages and includes the following action buttons:

- *Help*—additional window that displays the Help pages
- *Alerts*—pop-up window that displays the unread alerts
- *Change Password*—raises a dialog box for password change
- *Logout*—log out of the tool

The top banner includes the main menu, which contains the following selections:

- *Dashboard*—widgets that display information about the FortiPortal (FP)
- *Policy & Objects*—pages for viewing and modifying security policy, firewall objects and security profiles
- *View*—different views of the security event logs
- *Wireless Networks*—wireless networks, listed by site or by SSID
- *Reports*—lists of available reports
- *Rogue AP*—data about rogue APs
- *Additional Resources*—page to launch external pages such as a ticketing system
- *Audit*—a log of user activity on the Administrative Web Interface
- *Device Manager*—manage virtual private networks (VPNs) and static routes

The top banner also displays your storage usage, including the storage limit allocated and the actual amount of storage currently in use.

Landing page

When you open FortiPortal to login into the system, you see the following default landing page.


NOTE: With FortiPortal Version 3.2.1, you can now select German from this page.



Cloud Based Security Analytics and Management for Carriers and Managed Security Service Providers

Reset password

On the Login page, select the *Forgot password* link to display a dialog window:

Reset your password 

Please enter your email address and we will send you a temporary password

* Email:

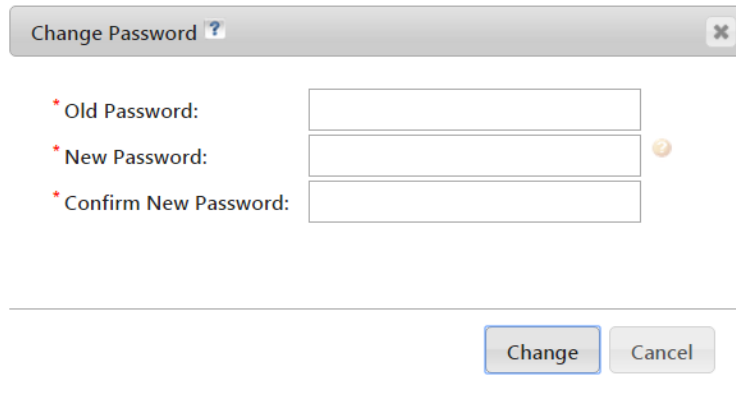
Send

Cancel

Enter the email ID associated with your user account. The system resets your password and sends you a temporary password by email.

Change Password

Selecting the Change Password icon on the page banner displays this dialog window:

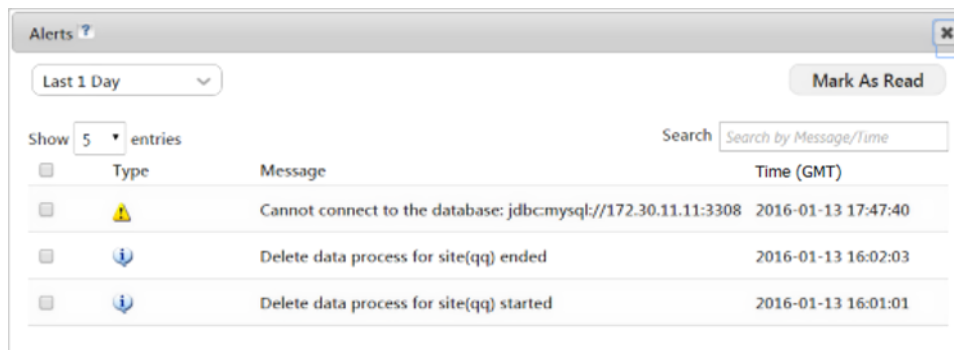


The dialog window has a title bar with the text "Change Password" and a question mark icon, and a close button (X) on the right. Below the title bar are three input fields with labels: "* Old Password:", "* New Password:", and "* Confirm New Password:". The "New Password:" label has a small yellow question mark icon to its right. At the bottom of the dialog are two buttons: "Change" and "Cancel".

Enter your existing password and a new password that takes effect on your next login attempt.

Alerts

Selecting the Alert icon displays a list of unread alerts:



For each alert, the page displays the following

- *Type*—severity of the alert (Informational or Warning)
- *Message*—text summary of the alert
- *Time*—time the alert was raised (displayed for GMT time zone).

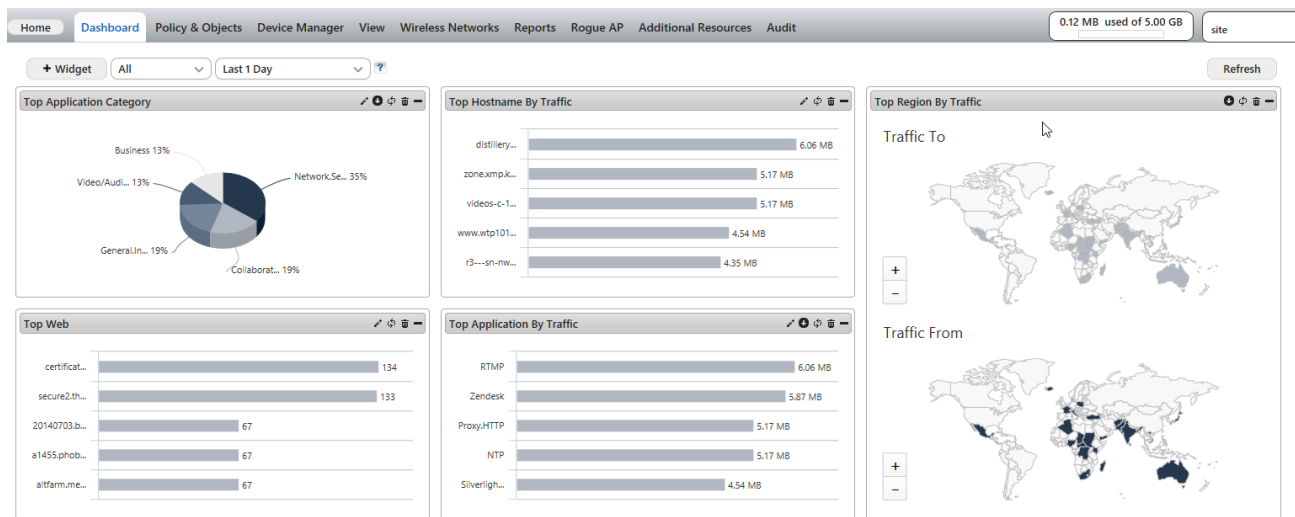
Page actions

The Alerts page contains the following actions:

- *Filter*—filter the data (Last 60 Minutes, Last 1 day, Last 1 week)
- *Search*—enter text to search for alerts containing that text
- *Show x Entries*—use the drop-down selector to set the number of entries to display
- *Select*—select individual alerts, or select all alerts (select box in the column header)
- *Mark as Read*—mark selected alerts as read

Dashboard

The dashboard displays different views of the security event logs and other information.



As you can see, the dashboard is organized as a set of widgets. The default widgets include the following:

- Top Application Category
- Top Hostname by Traffic
- Top Region by Traffic
- Top Web
- Top Application by Traffic
- Top Spam
- Traffic History
- Top Traffic By Protocol
- Top Viruses
- Top Attacks
- Top DLP Sources

The following widgets are associated with the wireless controllers and endpoints:

- Traffic History (Wireless)
- Top 5 FAPs by Max Client Count
- Top 5 FAPs by Max Bandwidth (Mbps)
- Max Client Count (Wireless)
- Top 5 SSIDs by Traffic (Wireless)
- FAP Summary

The following widgets are associated with the sandbox:

- Sandbox Scanning Statistics
- Top Sandbox Hosts

- Top Sandbox Malware
- Sandbox Scanning Statistics Graphs

Page actions

The following actions are available on the dashboard:

- **+ Widget**—add a widget to the dashboard
- **Scope**—view widget output (All, site, or wireless)
- **Filter**—filter the data (last hour, last day, last 7 days, or a custom filter)
- **Refresh**—refresh the data

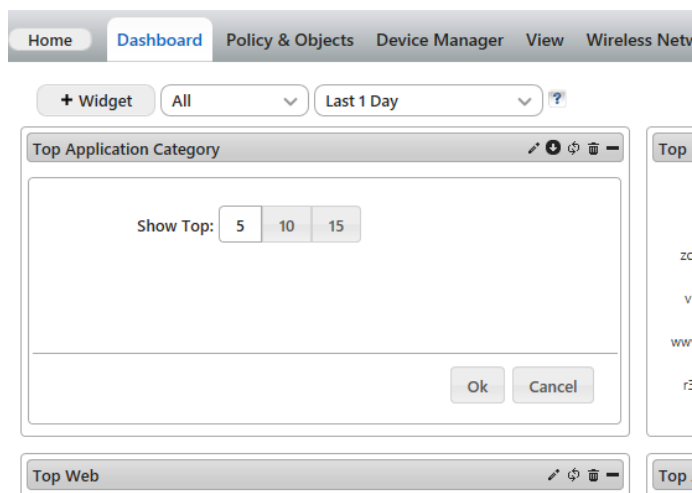
Widget actions

The top banner on each widget provides some or all of the following controls:

- **Edit Settings**—edit the widget
- **Drill-down**—visible in the widgets that support drill-down capability
- **Refresh**—refresh the data
- **Delete**—delete the widget
- **Collapse/Expand**—display or hide the widget's content
- **Drag and Drop**—using the menu bar

Edit widget

Selecting the Edit Settings icon opens a window within the widget that enables you to select the top N entries:

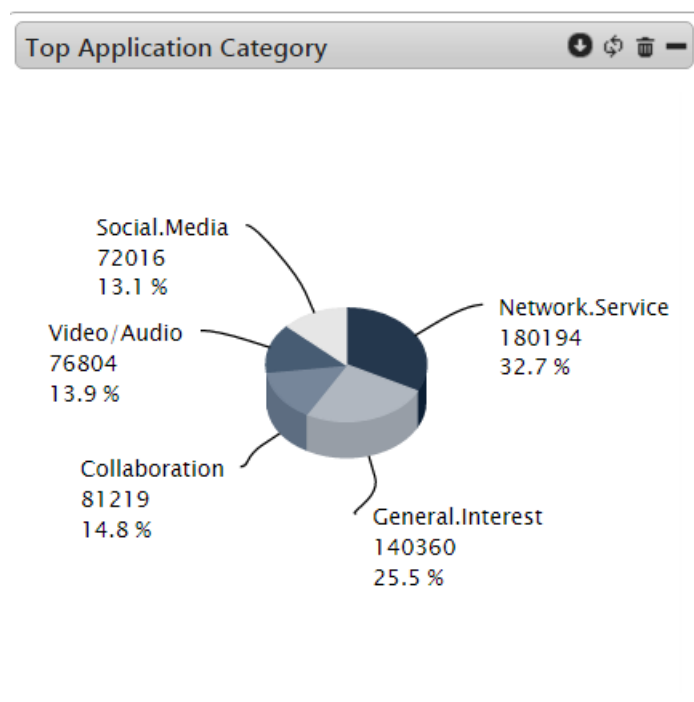


Drill-down widget

The following widgets support the drill-down capability:

- Top Application Category
- Top Region by Traffic
- Top Application By Traffic
- Top Attacks

Each of these widgets displays a graph or bar chart with the top 5 results, where the result is an application, region, traffic, or attack (depending on the widget). When you select one of the results, the Application view opens with a view filtered by that result. The view filter is listed above the table.



The application name in each table entry also displays the region name (in brackets).

View

This tab displays information about the security event logs. It contains filters and controls that allow you to group the event logs in different ways, and to drill down and view the details of a related set of event logs.

The following action buttons are available along the top of the page:

- *Application/Attack/Sandbox*—view the event logs grouped by application, attack or sandbox.
- *Scope*—view output for all sites or select a specific site
- *Set Filter*—filter the data (last hour, last day, last 7 days, or customize)
- *Refresh*—refresh the data
- *Sort*—Each column has a sorting feature, allowing you to sort data in ascending or descending order.

The table header provides a drop-down menu for selecting the number of entries to display. The header also includes a search box, enabling you to search for the text in the following fields: User, Source, Source Information (Src.Inf), Destination, Destination Information (Dst.Inf) and Application.

The following tabs provide different views of the data:

- *Source*—arranged by the source FortiGate device
- *Destination*—arranged by the destination (IP address, protocol, port)
- *Session*—arranged by session (i.e., a specific flow of packets between a source and destination). This tab is visible only when you have selected the Application view.

Application view

The *Application* tab under *View* displays event logs grouped by application:

Application Source Destination Session								
Show 10 entries	Search Search by Application (src) Country/Category/Risk							
Application Name	Category	Risk	# Users	# Source	# Destination	# Sessions	Bandwidth	
UserVoice (Kenya)	Business	Low	1	1	1	115	6.91 MB	
XiaoMLIM (Yemen)	Collaboration	high	1	1	1	115	12.92 MB	
Bing.Search (Saudi Arabia)	GeneralInterest	Low	1	1	1	116	5.15 MB	
Desktop.Weather (Nepal)	GeneralInterest	elevated	1	1	1	116	560.06 KB	
ESPN.SportsCentre (Thailand)	GeneralInterest	Low	1	1	1	116	5.69 MB	
Kerberos (New Zealand)	Network.Service	high	1	1	1	116	1.35 MB	
MS.RPC (Japan)	Network.Service	medium	1	1	1	116	1.15 MB	
Rss (Taiwan)	Network.Service	Low	1	1	1	117	1.33 MB	
SNMP_GetRequest (Ukraine)	Network.Service	Low	1	1	1	116	4.85 MB	
Facebook (France)	Social.Media	Low	1	1	1	115	7.26 MB	

Note the name (in brackets).

Attack view

The **Attack** tab under **View** displays event logs grouped by "attack:"

Attack	Source	Destination	Log
Show 10 entries			
Attack Name	Count	Level	Severity
ASUS.Net4Switch.Ipssec.ActiveX.Stack.Buffer.Overflow	116	alert	alert
Adobe.Flash.Player.copyRawDataToMemory.Corruption	116	alert	alert
Apple.QuickTime.MPEG.Stream.Padding.Buffer.Overflow	116	alert	alert
Cisco.CSdv50135.Telnet.Buffer.Overflow	116	alert	alert
EMC.Data.Protection.Advisor.DoS	116	alert	alert
HP.Intelligent.Management.Center.ssm.exe.Buffer.Overflow	116	alert	alert
HPE.HPEInc.Remote.File.Inclusion	116	alert	alert
Kordil.Arbitrary.File.Upload	116	alert	alert
MS.Help.Program.DoS	116	alert	alert
MS.Windows.RDP.Remote.Code.Execution	116	alert	alert

When you select one of the entries in the table, the system displays the first set of filtering. For each of the remaining filters, a vertical left menu includes buttons to perform the next level of filtering (see **circle 1** below):

Attack ▾ All ▾ Last 60 Minutes ▾ ? Refresh

Attack Source Destination Log

Attack (3D.Life.Player.WebPlayer.ActiveX.Control.Buffer.Overflow) Source (172.30.184.124)

Destination Log

Show 10 entries Search Search by Destination

#	Destination	# Logs
1	157.56.52.41	1

The applied filters are listed across the display (**ellipse 2** in the preceding figure). Select the grey x button beside each filter to remove that filter.

If you select an individual log entry, the system displays its details:

Application

Source

Destination

Session

Source (172.30.1.10 (FORTINET-USchernandez))

Application (NetBIOS.Name.Service)

Destination (157.55.130.140)

Session

Show 10 entries

Search Search by User/Source/Src.Inf./Destination/Dst.Inf./Application

#	Time	User	Source	Src.Inf.	Destination	Dst.Inf.	Application Name	Bandwidth	Policy ID
<div> <div></div> <div>1</div> </div>	2016-01-21 11:38:11	FORTINET-USchernandez	172.30.1.10	internal	157.55.130.140	root	NetBIOS.Name.Service	41.75 KB	8

To the left of the entry, the system provides an expand button to display all of the fields associated with the log entry.

Sandbox view

The *Sandbox* tab under *View* displays event logs grouped by “sandbox:”

Sandbox ▾

All ▾

Last 7 days ▾

?

Refresh

Sandbox

Source

Destination

Log

Show 10 ▾ entries

Search

Malware Name	Risk	Level	Client Device Id	# Users	# Source	# Destination
BSIL/RVX!nr	Low Risk	alert	FGT20C1021119MDL	348	196	250
CSIL/AVX!cr	High Risk	alert	FGT20C1021119MDL	336	196	250
DSIL/cVX!dr	Medium Risk	alert	FGT20C1021119MDL	346	195	247
ESIL/dVX!dr	Clean	alert	FGT20C1021119MDL	340	196	248
FSIL/eVX!dr	High Risk	alert	FGT20C1021119MDL	345	195	246
GSIL/fVX!dr	unknown	alert	FGT20C1021119MDL	346	196	248
MSIL/MVX!tr	Malicious	alert	FGT20C1021119MDL	343	195	248
zSIL/hVX!dr	Malicious	alert	FGT20C1021119MDL	342	196	246

Use the *Source* or *Destination* tab to filter the view. The *Log* tab shows the logs unfiltered.

When you select one of the entries in the table, the sandbox view works like the attack view. The system displays the first set of filtering. For each of the remaining filters, a vertical left menu includes buttons to perform the next level of filtering.

The applied filters are listed across the display. Select the grey x button beside each to remove that filter.

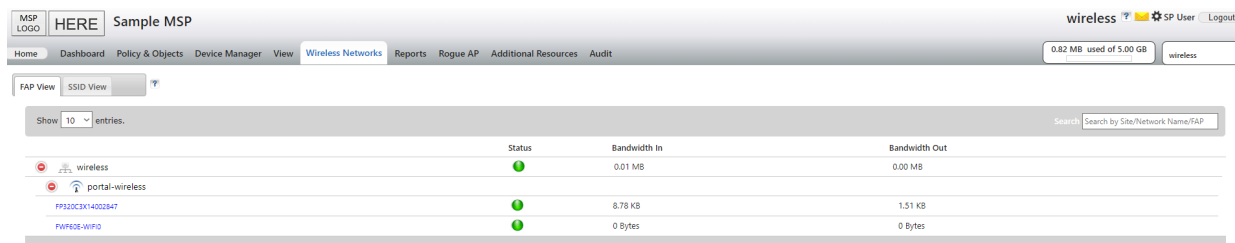
If you select an individual log entry, the system displays the details of that entry.






Wireless Networks

This tab displays information about the wireless networks.

You can select from two views, Fortinet Access Points (FAP) and SSID, which present the same information grouped in different ways:

- **FAP View**—displays the SSIDs for each FAP at each site (see the following figure)
- **SSID View**—displays the FAPs for each site for each SSID



	Status	Bandwidth In	Bandwidth Out
 wireless		0.01 MB	0.00 MB
 portal-wireless		8.78 KB	1.51 KB
FW900-WIFI		0 Bytes	0 Bytes

Selecting the green + button adjacent to an entry expands the entry and shows the next level of data. Select a red button to hide the data for an entry.


If you select the FAP name, the system opens a window to show the FAP details as well as details for each SSID.

Additional information about Fortinet Wireless networks is available in the [wireless chapter](#) of the FortiOS handbook.

Reports

This tab displays a list of available FortiPortal or FortiAnalyzer reports:

FortiPortal
FortiAnalyzer

Today


Show 10 entries

Created (GMT)	Date Range (GMT)	Report Name
2018-05-24 20:49:25	2018-05-23 20:49:25 / 2018-05-24 20:49:25	Report_MME_1527194965542.pdf

FortiPortal reports

The FortiPortal reports page includes the following actions:



- *Set Filter*—filter the data (today, last 1 day, last 1 week, last 1 month, or customize a filter)
- *Report Definitions*—opens a pop-up window that lists the available reports
- *Run Now*—opens a pop-up window with a form to specify the report to be run
- *Search*—text search by report name

NOTE: The *Report Definitions* and *Run Now* buttons are visible only to users with the relevant permissions.

When you scroll over a entry in the reports table, the following icons appear in the Action column:

- *Download*—download the selected report
- *Delete*—delete the selected report

Report definition actions

Reports 


+ Add

Search

Report Name	User Type	Frequency	Site	Action
cust1rep	CUST	Daily	All	
cust1rep2	CUST	Weekly	aa	
Custrep1	SP	Weekly	All	
Report1	SP	Daily	aa	

The Report Definitions form contains the following actions:

- *Add*—open a new page with the form to add a report
- *Search*—enter text to search for report names containing that text

Run Now actions

The Run Now form contains the following selections:

Settings	Guidelines
Report Duration	Duration of data included in the report: last 1 day, last 1 week, last 1 month
Available/Selected Reports	Use the arrow keys to create a subset of available reports.
Available/Selected Sites	Use the arrow keys to create a subset of available sites. If none are selected, the report is run for all sites.
Language	Language for the report selected from the pull-down list
No of Rows	Number of rows of data to include in the report

Per-report actions

When you scroll over a entry in the reports list, the following icons appear in the Action column:

- *Edit*—opens a new page with the form to edit the selected report
- *Delete*—deletes this report

The Add Report and Edit Report forms contain the following selections:

Settings	Guidelines
Report Name	Name for the report
Frequency	Values include: daily, weekly, monthly
Available/Selected Reports	Use the arrow keys to create a sublist of available reports. Use the search boxes to filter the choices available.
Available/Selected Sites	Use the arrow keys to create a sublist of available sites. (If none are selected, the report is run for all sites.) Use the search boxes to filter the choices available.
Language	Language for the report from the pull-down list
No of Rows	Number of rows of data to include in the report

Settings	Guidelines
From Email	Email address from which the report will be sent
Email Text	Text for the body of the email

FortiAnalyzer reports

When you select the *FortiAnalyzer* tab, the FortiPortal displays a reports page:

FortiPortal FortiAnalyzer

Last 1 Month ?

Show 10 entries Search Search by Report Name

Created (GMT)	Report Name	Action
2016-08-22 21:16:31	f1/root/Admin and System Events Report-2016-08-22-1416	

This page includes the following actions:

- **Set Filter**—filter the data (today, last 1 day, last 1 week, last 1 month, or customize a filter).
- **Search**—text search by report name

When you scroll over a entry in the reports table, the following icon appears in the Action column:

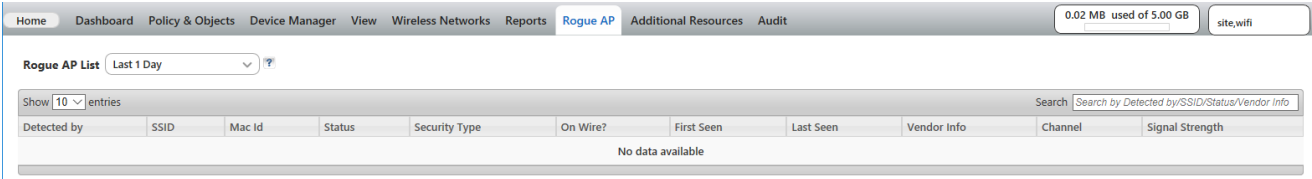
- **Download**—downloads the selected report as a PDF file

Rogue AP

This tab displays a list of rogue access points detected on the network and contains the following actions

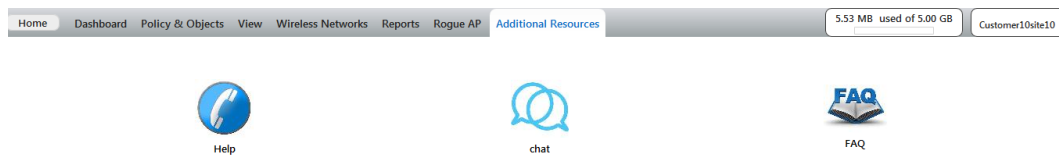
- *Set Filter*—filter the data (last 60 Minutes, last 1 day, last 7 days, or customize a filter)
- *Show x entries*—drop-down menu to set the number of entries per page
- *Search*—search the fields: Detected by, SSID, Status, Vendor information

The following figure shows the Rogue AP page:



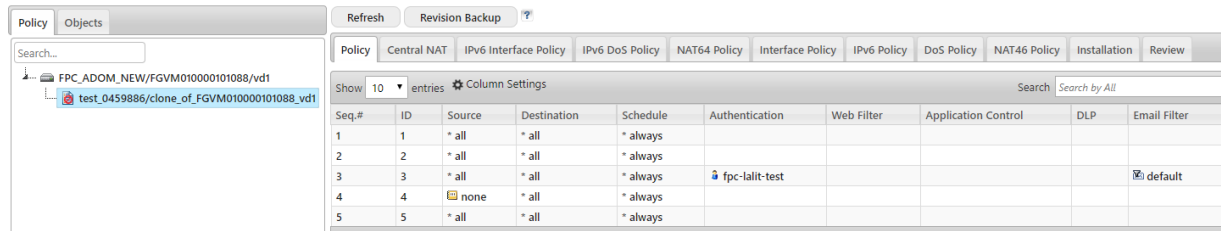
Additional Resources

This tab displays Help, Chat, and FAQ buttons. If active, the button's text and image are selectable and open a new tab with the given URL. If disabled, the button's text and image cannot be selected.



Policy

Go to *Policy & Objects > Policy* to see a hierarchical view of the policy packages. Each package might be associated with either one or more FortiGate devices or VDOMs, or all devices within an ADOM.



The page includes a main panel and a left side panel that provides a hierarchical view of the policies. When you select an entry in the left panel, the main panel displays the policy data associated with that entry.

Policy tab column settings

You can select the columns to display in the *Policy* tab:

1. Select the *Column Settings* button to display the Column Settings form.
2. Select the columns you want to display, clear the columns that you want to hide, and select *Apply*.

Policy data refresh

The policy information is refreshed every hour from the FortiManager. You can also refresh the data on demand by selecting the *Refresh* button.

Revision backup

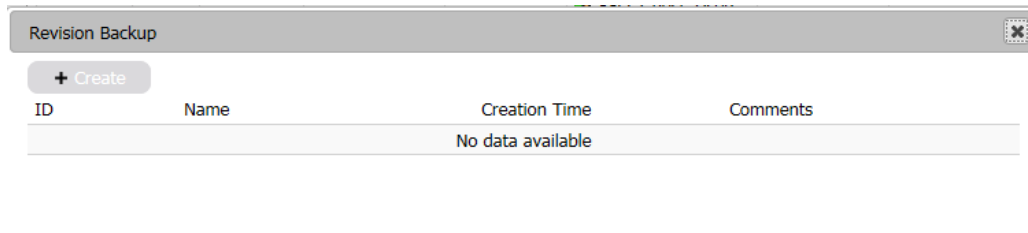
The system can save only one revision of the current policy and object data. The new revision overwrites the existing backup (if one exists).

Observe the following restrictions:

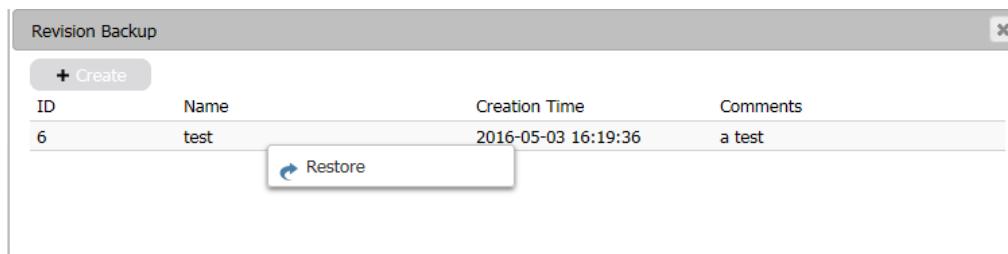
- Customer must be part of only one ADOM.
- No other customer can be part of that ADOM.

Creating and restoring policy revisions

Select the *Revision Backup* button to open the Revision Backup window:



Select the *Create* button to define a backup of the current policy and object data. If one exists, the Revision Backup window provides details:



To restore the backup, right-click the entry and select *Restore*.

Configuring policies

Your service provider can grant write access to your policies. If so, you are enabled to add/edit/delete, enable/disable, and change the order of the policies. If not, we display a warning message and restrict the data in the Policy page to read-only.

Adding a new policy

1. Right-click a policy in the list and select *Create New*.
2. Enter values in the relevant fields and select *Save*.

Updating a policy

1. Right-click the policy in the list and select *Edit*.
2. Modify the relevant fields and select *Save*.

Deleting a policy

1. Right-click the policy in the list and select *Delete*.

Enabling or disabling a policy

1. Right-click the policy in the list and select *Enable* or *Disable*.
A policy in disabled state is marked with a red circle in the Seq.# column.

Policy fields

The add/edit policy form contains the following fields (see the figure after the table for an example form):

Settings	Guidelines
Policy Subtype	Address or User Identity
Incoming Interface	Select one or more interfaces from the drop-down list.
Source Address	Select to add one or more address objects.
Outgoing Interface	Select one or more interfaces from the drop-down list.
Destination Address	Select to add one or more address objects.
Schedule	Select one entry from the drop-down list.
Service	Select one or more services from the drop-down list.
Action	Accept or deny.
Tags	You can add tags for tag management. Type a tag in the text field and select the add icon to apply the tag to the policy.
Comments	Type optional comments for the policy.
Additional field becomes visible if the action is set to Deny	
Log Violation Traffic	Select this check box to create a log for each denied packet.
Additional fields become visible if the action is set to Accept	
NAT	
Use Destination Interface Address	Select to use the destination interface address. This setting is enabled by default. Optionally, enable Fixed Port.
Dynamic IP Pool	If you check this option, specify the IP pool to use.
Use Central NAT Table	Uses the central NAT table for source IP mapping.
Logging Options	Logging Options

Settings	Guidelines
No Log	No log is generated.
Log Security Events	Creates a log for each security event.
Log All Sessions	Logs all sessions. Requires extensive system resources and storage space.
Other Options	
Enable Web Cache	Enable web caching for this traffic.
Enable WAN Optimization	Enable WAN Optimization for this traffic.
Enable Disclaimer	Enable Disclaimer for this type of traffic.
Redirect URL	Configure the redirect URL of the disclaimer.
Resolve User Names Using FSSO Agent	Authenticate user credentials with FortiAuthenticator.
Security Profiles	Enable one or more security profiles for this traffic.
Traffic Shaping	Apply traffic shaping to this traffic. The amount of shaping applied depends on the traffic priority that you configure (Guarenteed, High, Medium, Low).
Reverse Direction Traffic Shaping	Apply traffic shaping to the traffic coming in the reverse direction.
Per-IP Traffic Shaping	Apply the traffic shaping per-IP.

The following figure shows the Create New Policy form:

Create New Policy
✕

Groups(s) Click to add...

User(s) Click to add...

Source Device Type Click to add...

Incoming Interface * any

Source Address * all ✓

Outgoing Interface * any

Destination Address * all ✓

Schedule always

Service ALL ✓

Action DENY

☒ Log Violation Traffic

Tags

Add tags Click to add...

Comments Write a comment... 0/1023

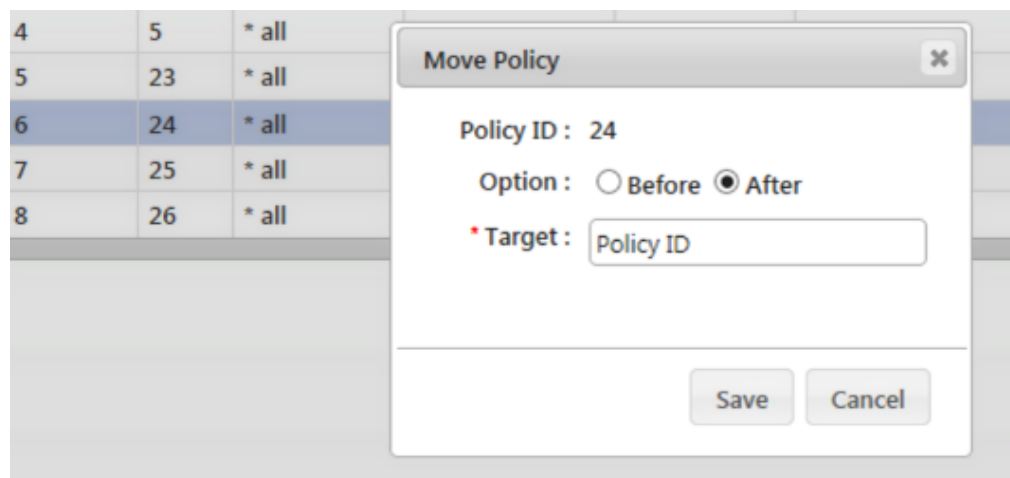
Save Cancel

Moving a policy

NOTE: Policy move is not supported for FortiManager 5.4.0 or later release.

To change the order of the policies:

1. Right-click the policy in the list and select *Move*.
The system opens a dialog box, showing the policy ID of the selected policy.
2. Select the option of *Before* or *After*.
3. Enter the target Policy ID (**NOTE: Enter the ID, NOT the sequence number**).
The system moves the selected policy to before/after the target.



Re-installing the policy

After you add or change a policy, select *Installation* to view the installation targets. Right-click a target and select *Re-install* to re-install the policy packages to the assigned devices.

For additional information about policy types, refer to the chapter on Policy and Objects in the [FortiManager Administrative Guide](#).

Reviewing policies

Go to *Policy & Object > Policy > Review* to see all policies and firewall objects that have been configured.

Refresh
Revision Backup

Policy
Installation
Review

Max Rules Per Page: 10
Print

Seq.	ID	Source Interface	Destination Interface	Source	Destination	Schedule	Authentication	Web Filter	Application Control	DLP	Email Filter
1	1	port8	port9	net-10-50-20	* all	* always					

Address

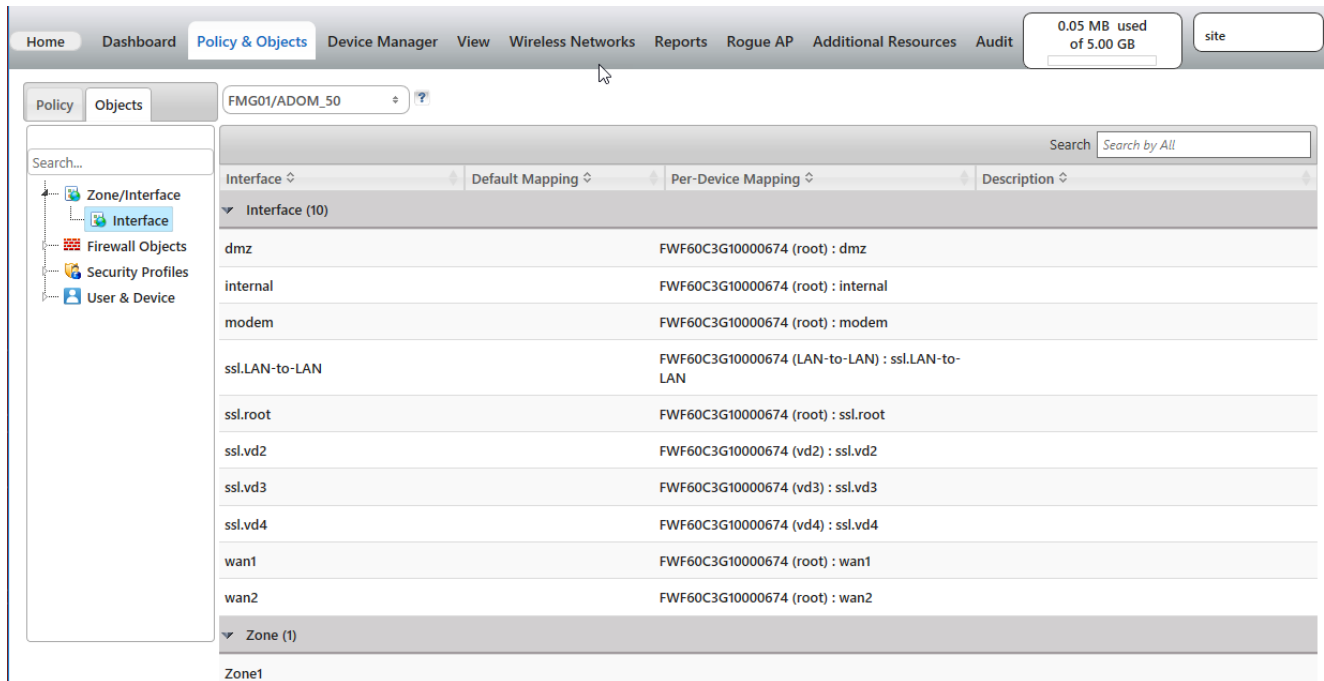
Name	Type	Interface	Default Mapping	Comments
.live.com	Address	any	FQDN:.live.com	
Adobe Login	Address	any	FQDN:*.adobe.com	
Gotomeeting	Address	any	FQDN:*.gotomeeting.com	
SSLVPN_TUNNEL_ADDR1	Address	any	IP Range:10.212.134.200-10.212.134.210	
SSLVPN_TUNNEL_IPv6_ADDR1	IPv6 Address		IP/Netmask::ffff::/120	
Windows update 2	Address	any	FQDN:*.windowsupdate.com	
adobe	Address	any	FQDN:*.adobe.com	
all	Address	any	IP/MASK:0.0.0.0/0.0.0.0	
all	IPv6 Address		IP/Netmask:::/0	
android	Address	any	FQDN:*.android.com	
apple	Address	any	FQDN:*.apple.com	
appstore	Address	any	FQDN:*.appstore.com	
auth.gfx.ms	Address	any	FQDN:auth.gfx.ms	
autoupdate.opera.com	Address	any	FQDN:autoupdate.opera.com	
citrix	Address	any	FQDN:*.citrixonline.com	
dropbox.com	Address	any	FQDN:*.dropbox.com	
ease	Address	any	FQDN:*.ease.com	
firefox update server	Address	any	FQDN:aus*.mozilla.org	
fortinet	Address	any	FQDN:*.fortinet.com	
google-drive	Address	any	FQDN:*.drive.google.com	
google-play	Address	any	FQDN:*.play.google.com	
google-play2	Address	any	FQDN:*.gplay.google.com	

You can select the maximum number of rules to display.

Select *Print* to send the information to a printer or to create a PDF file.

Objects

This tab under *Policy & Objects* provides a view of the objects that are defined in the FortiManager devices. Objects can include items such as addresses, services, intrusion protection definitions, anti-virus signatures and web-filtering profiles. You can use an object in more than one policy to avoid repeating data in multiple places.



Interface	Default Mapping	Per-Device Mapping	Description
Interface (10)			
dmz		FWF60C3G10000674 (root) : dmz	
internal		FWF60C3G10000674 (root) : internal	
modem		FWF60C3G10000674 (root) : modem	
ssl.LAN-to-LAN		FWF60C3G10000674 (LAN-to-LAN) : ssl.LAN-to-LAN	
ssl.root		FWF60C3G10000674 (root) : ssl.root	
ssl.vd2		FWF60C3G10000674 (vd2) : ssl.vd2	
ssl.vd3		FWF60C3G10000674 (vd3) : ssl.vd3	
ssl.vd4		FWF60C3G10000674 (vd4) : ssl.vd4	
wan1		FWF60C3G10000674 (root) : wan1	
wan2		FWF60C3G10000674 (root) : wan2	
Zone (1)			
Zone1			

The page includes a main panel and a left side panel that provides a hierarchical view of the objects. When you select an object in the left menu, the main panel displays the data associated with that object. This data is displayed for the selected ADOM. You can select a different ADOM using the pull-down selector above the main panel.

Types of objects

The page displays the following object categories:

- Zone/Interface
- Firewall Objects
- Security Profiles
- User & Device

These objects are described in the following sections.

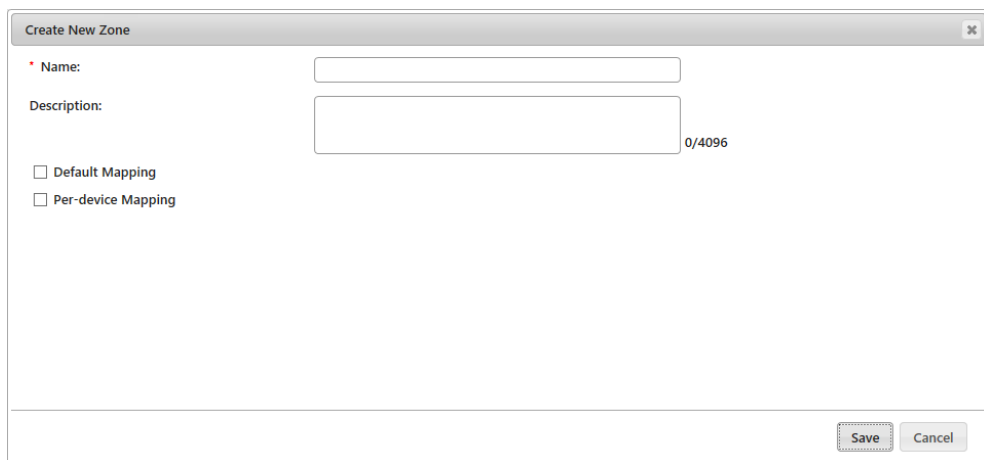
Zone/Interface

You can define a dynamic interface or a dynamic zone. A dynamic zone allows you to specify multiple interfaces.

The following figure shows the Create New Interface form.



The following figure shows the Create New Zone form.



Specify the name of the dynamic interface or zone, add an optional description, and select one of the default mappings. You can also specify dynamic mapping for a device by selecting *Per-Device Mapping*.

Firewall Objects

Firewall objects include address, schedule, service and virtual IP. For additional information about the object types, see [FortiOS 5.6 Object Configuration](#).

Address

You can specify an address as a country, an FQDN or as an IP subnet and mask. The address can apply to all interfaces, or you can configure a specific interface.

You can also create an Address Group, which defines a group of related addresses.

Schedule

You can specify a set of days and time ranges with recurring or one-time schedules.

Service

Although numerous services are already configured, the system allows for administrators to configure their own.

The service object specifies the protocol and any additional information required to identify the service (which depends on the protocol):

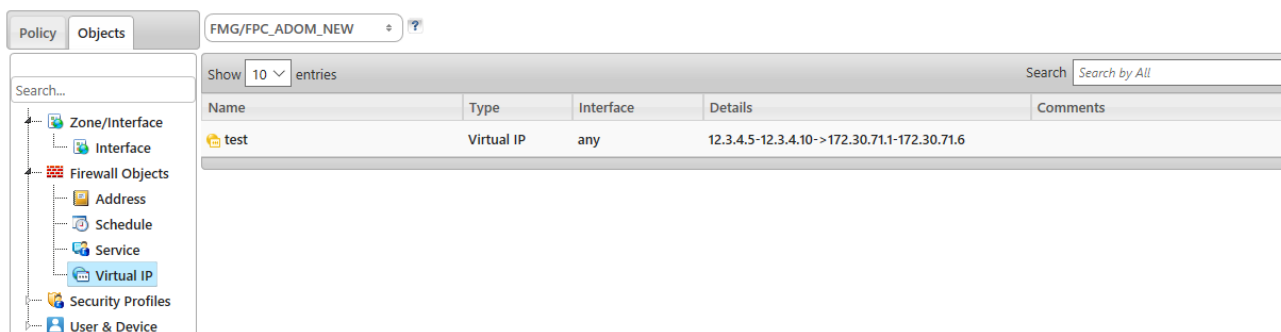
- *IP*—IP protocol number
- *TCP/UDP/SCP*—source and destination port range

You can also create a service group, which defines a group of related services.

Virtual IP

The Virtual IP objects map external IP addresses to internal addresses.

The following figure shows the FPC Virtual IP object display:



FPC supports the following Virtual IP object types:

- *IPv4 Virtual IP*—uses static NAT to map a range of external addresses to an internal address range
- *IPv4 Virtual IP Group*—defines a group of one or more Virtual IPs, for ease of administration
- *IP Pool*—defines an IP address or range of IP addresses to use as the source address (rather than the IP address of the interface)

Security Profiles

Security profiles are described in detail in the [FortiGate Security Profiles](#) document and in the online help files at [FortiOS Security Profiles](#).

The following security profiles are supported on an FPC:

- Antivirus Profile
- Application Sensor
- Data Leak Prevention Sensor
- Email Filter Profile
- IPS Sensor
- Web Filter Profile
- Local Category
- Rating Overrides

Local Category (security profile introduced with FPC 1.2.0)

You can create a local category and then use Rating Override to assign URLs to the new category.

Rating Overrides (security profile introduced with FPC 1.2.0)

Use a Rating Override object to override the Fortinet rating for a URL. The [Security Profiles](#) document contains additional information about local categories and rating overrides.

The following figure displays rating overrides:

The screenshot shows the FortiGate web interface. On the left, the 'Objects' tab is selected, and the 'Rating Overrides' object is highlighted in the tree. The main panel shows a table of rating overrides for the policy 'FMG/FPC_ADOM_NEW'.

URL	Status	Category
http://www.google.com:8080/business	enable	Brokerage and Trading
www.google.com/a	enable	Finance and Banking
www.hey.com	enable	Phishing
www.nogo.com	enable	Peer-to-peer File Sharing

User & Device

Security policies may allow access to specified users and user groups only (the object types in the User & Device category).

For additional information about users and user groups, refer to [FortiOS Handbook: Authentication](#).

User Definition

You can create local (accounts stored on the FortiGate unit), or remote users (accounts stored on a remote authentication server). FortiGate supports LDAP, RADIUS, and TACACS+ servers.

You can also enable two-factor authentication using FortiAuthenticator.

The following figure shows the Edit User form for a local user:

The screenshot shows the 'Edit User Profile: guest' form. At the top, the title bar says 'Edit User Profile: guest' with a close button. The form has several sections:

- Type:** Radio buttons for LOCAL (selected), LDAP, RADIUS, and TACACS+.
- User Name:** A text field containing 'guest'.
- Password:** A text field with masked characters (dots). A checkbox labeled 'Disable' is checked.
- Contact Info:** A checkbox for 'Email' is unchecked, followed by an empty text field.
- Enable Two-factor Authentication:** A checkbox is unchecked. Below it, radio buttons for 'FortiToken' (selected) and 'Email based two-factor authentication' are shown. Under 'FortiToken', there is a button labeled 'Click to add...'.

At the bottom right of the form, there are 'Save' and 'Cancel' buttons.

For a remote user, you need to specify the remote server, as shown in the following figure:

The screenshot shows the 'Edit User Profile: fpcrduser' form. The title bar says 'Edit User Profile: fpcrduser' with a close button. The form has several sections:

- Type:** Radio buttons for LOCAL, LDAP, RADIUS (selected), and TACACS+.
- User Name:** A text field containing 'fpcrduser'.
- Disable:** A checkbox is unchecked.
- RADIUS:** A text field containing 'Test_radius'.
- Contact Info:** A checkbox for 'Email' is unchecked, followed by an empty text field.
- Enable Two-factor Authentication:** A checkbox is unchecked. Below it, radio buttons for 'FortiToken' (selected) and 'Email based two-factor authentication' are shown. Under 'FortiToken', there is a button labeled 'Click to add...'.

At the bottom right of the form, there are 'Save' and 'Cancel' buttons.

User Group

A user group is a list of user identities. To add or edit a user group, right-click the Edit Settings icon to display the Edit User Group form. Then, select group members from the *Available Users* list.

After you set the group type and add members, you cannot change the group type without removing its members. If you change the type, any members will be removed automatically.

Group Name:

Type: ☒ Firewall ☐ FSSO

Available Users: abc, fpcrduser, testRdUser

Members: guest

Remote authentication servers

+ Create New

Remote Server	Group Name
No data available	

Save Cancel

Configuring objects

Your service provider may grant write access to some or all of your policy objects. If so, you are enabled to add/edit/delete the objects displayed on the page. If not, we display a warning and set the data to read-only.

Adding a new object

1. Right-click any object in the list and select *Create New*.
2. Modify the relevant fields and select *Save*.

Updating an object

1. Right-click the object in the list and select *Edit*.
2. Modify the relevant fields and select *Save*.

Deleting an object

1. Right-click the object in the list and select *Delete*.
2. Modify the relevant fields and select *Save*.

If the new or updated object is used in any policy, select *Installation* in the *Policy* tab to re-install the policy packages to the assigned devices.

Audit

The Audit tab displays an log of user activity on the administrative web interface:

Home

Dashboard

Policy & Objects

Device Manager

View

Wireless Networks

Reports

Rogue AP

Additional Resources

Audit

0.02 MB used of 5.00 GB

site

Audit Log List

Last 1 Day

Export to CSV

Show10▼entries

Search

Search by Level/User Name/Event Type/Client IP Address/Mess

Date (US/Pacific)	Level	User Name	Event Type	Client IP Address	Message
2017-11-20 15:24:52	info	spuser	Edit Object	172.30.180.226	Object type: webfilter-profile ObjectName/Id: Mantis457764 edited for adom: ADOM_50
2017-11-20 15:24:00	info	spuser	Add Object	172.30.180.226	Object type: webfilter-profileObject Name: created for adom: ADOM_50
2017-11-20 15:08:20	info	spuser	Add Object	172.30.180.226	Object type: ratingoverridesObject Name: created for adom: ADOM_50
2017-11-20 15:07:53	info	spuser	Add Object	172.30.180.226	Object type: localcategoryObject Name: created for adom: ADOM_50
2017-11-20 15:07:30	info	spuser	Add Object	172.30.180.226	Object type: webfilter-profileObject Name: created for adom: ADOM_50
2017-11-20 15:06:47	info	spuser	Delete Object	172.30.180.226	Object type: localcategory ObjectName/Id: myLocalCategory deleted for adom: ADOM_50
2017-11-20 15:06:27	info	spuser	Delete Object	172.30.180.226	Object type: webfilter-profile ObjectName/Id: test 101 deleted for adom: ADOM_50
2017-11-20 14:55:52	info	spuser	Delete Object	172.30.180.226	Object type: webfilter-profile ObjectName/Id: Test after fix deleted for adom: ADOM_50
2017-11-20 14:55:46	info	spuser	Delete Object	172.30.180.226	Object type: webfilter-profile ObjectName/Id: My test web filter deleted for adom: ADOM_50
2017-11-20 14:55:39	info	spuser	Delete Object	172.30.180.226	Object type: webfilter-profile ObjectName/Id: myWebFilterProfile deleted for adom: ADOM_50

Showing 1 to 10 of 11 entries

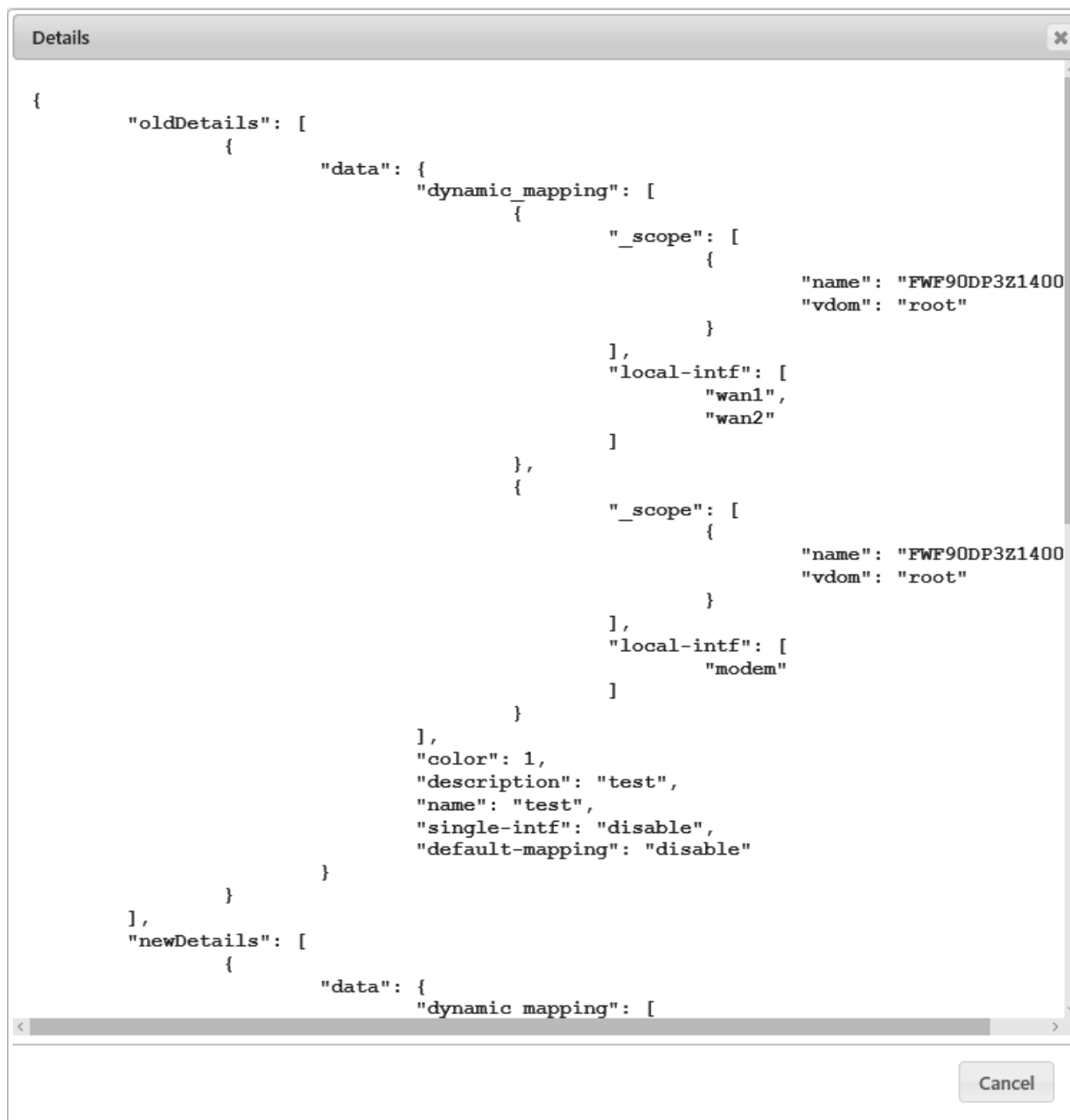
FirstPrevious12NextLast

Page actions

- *Audit Log List*—set the duration of the logs to display (last 60 minutes, last 1 day, last 7 days, or customize)
- *Search*—use any column to search the audit log list by level, user name, event type, client IP address, or message
- *Export to CSV*—export the audit log list as a Comma-Separated Value (CSV) file

Per-audit actions

When you select the *Message* field for an *Edit Customer* audit entry, the system opens a pop-up window to display the details of the change. The details window shows the original ("oldDetails") and new ("newDetails") field values:



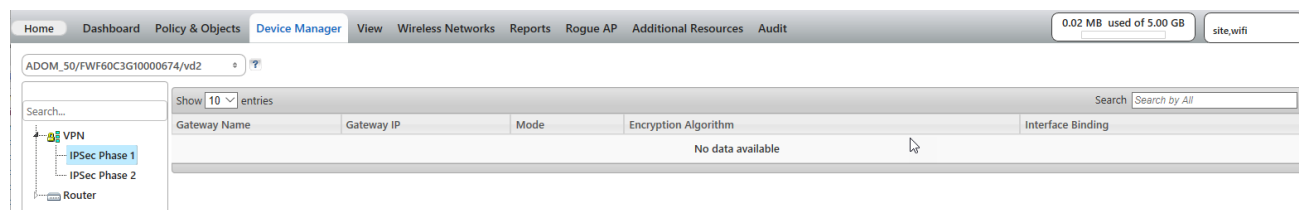
Device Manager

Use the Device Manager tab for the following:

- [Configure IPSec phase 1 and phase 2.](#)
- [Define static routes.](#)

VPNs ?

The VPN tree under the Device Manager tab displays a list of configurations for Internet Protocol Security (IPSec) Phase 1 and Phase 2.



Configuring VPNs

Use the VPN area to configure IPSec phase 1 and phase 2. You must have at least one IPSec phase-1 configuration and at least one IPSec phase-2 configuration.

In this area, the following actions are available:

- **Search**—enter text to search for in the table
- **Create New**—configure the IPSec phase 1 or the IPSec phase 2
- **Edit**—change an existing IPSec phase-1 or IPSec phase-2 configuration
- **Delete**—delete an IPSec phase-1 or IPSec phase-2 configuration

Creating an IPSec phase-1 or phase-2 configuration

1. Select *IPSec Phase 1* or *IPSec Phase 2* from the VPN tree.
2. Right-click a configuration and select *Create New*. If the table is blank, right-click under the column headings and select *Create New*.
3. Enter values in the relevant fields and select *Save*. See "IPSec phase-1 fields" on page 169 and "IPSec phase-2 fields" on page 171.
4. Select *Save*.

Updating an IPSec phase-1 or phase-2 configuration

1. Select *IPSec Phase 1* or *IPSec Phase 2* from the VPN tree.
2. Right-click a configuration and select *Edit*.
3. Update the values that have changed.
4. Select *Save*.

Deleting an IPSec phase-1 or phase-2 configuration

1. Select *IPSec Phase 1* or *IPSec Phase 2* from the VPN tree.
2. Right-click a configuration and select *Delete*.

IPSec phase-1 fields

Create New IPSec Phase1

* Gateway Name:
The Gateway Name field is required.

Comments: 0/255

* Remote Gateway:

* IP Address:

* Local Interface:

* Mode: ☒ Main ☐ Aggressive

* Authentication Method: ☒ Pre-shared Key ☐ Signature

* Pre-shared Key:
The Pre-shared Key field is required.

The Create New IPSec Phase1 and Edit IPSec Phase1 forms contain the following fields:

Settings	Guidelines
Gateway Name	Required. Type a name for this Phase-1 configuration. The value is a string with a maximum of 15 characters.
Comments	Type an optional description. The value is a string with a maximum of 255 characters.
Remote Gateway	Required. Select <i>Static IP Address</i> , <i>Dialup user</i> , or <i>Dynamic DNS</i> .
IP Address	Required if you select <i>Static IP Address</i> . Type the IPv4 address.
Dynamic DNS	Required if you select <i>Dynamic DNS</i> . Type the fully qualified domain name.
Local Interface	Required. Select an interface from the drop-down list or select <i>any</i> .
Mode	Required. Select <i>Main</i> or <i>Aggressive</i> for the phase-1 mode.
Authentication Method	Required. Select <i>Pre-shared Key</i> or <i>Signature</i> for the authentication method.
Pre-shared Key	If <i>Pre-shared Key</i> is selected, this field is required. Type a string for the pre-shared key. The key must contain at least 6 printable characters. For optimum protection against currently known attacks, the key must consist of a minimum of 16 randomly chosen alphanumeric characters.

Settings	Guidelines
User Group	If <i>Pre-shared Key</i> is selected, this field is available but optional. Enter the user group to authenticate remote VPN peers. The user group can contain local users, LDAP servers, and RADIUS servers.
Certificate Name	If <i>Signature</i> is selected, this field is available but optional. Select a certificate from the drop-down list.
Peer Options	If <i>Signature</i> is selected, this field is available but optional. Select <i>Any peer id</i> or <i>One peer id</i> .
peer id	If <i>One peer id</i> is selected, this field is required. Enter the peer ID to uniquely identify one end of a VPN tunnel, enabling a more secure connection. If you have multiple VPN tunnels negotiating, this ensures the proper remote and local ends connect. The value is a string with a maximum of 255 characters.
Advanced...(XAUTH, NAT-traversal, DPD)	
Local Gateway IP	Select <i>Specify</i> or <i>Main Interface IP</i> . If you select <i>Specify</i> , type the IPv4 address in the field.
P1 Proposal	Select the encryption and authentication algorithms. You can select more than one. Use the arrows to move the algorithms from Available Encryption-Authentication Pair box to the Selected Encryption-Authentication Pair box.
Diffie-Hellman Groups	Select one or more of the following Diffie-Hellman (DH) groups: 2, 5, 14, 15, 16, 17, 18, 19, 20, 21. At least one of the DH group settings on the remote peer or client must match one the selections on the FortiGate unit. Failure to match one or more DH groups will result in failed negotiations. Only one DH group is allowed for static and dynamic DNS gateways in aggressive mode. By default, 5 and 14 are selected.
Key Life	Type the time (in seconds) that must pass before the IKE encryption key expires. When the key expires, a new key is generated without interrupting service. The key life can be from 120 to 172800 seconds. The default is 86400.
Local ID	A Local ID is an alphanumeric value assigned in the Phase 1 configuration. The Local ID uniquely identifies one end of a VPN tunnel, enabling a more secure connection. If you have multiple VPN tunnels negotiating, this ensures the proper remote and local ends connect. Type a string with a maximum of 63 characters.
XAuth	Select <i>Disable</i> or <i>Client</i> for the XAUTH type. The default is <i>Disable</i> .
NAT-traversal	Select <i>Disable</i> , <i>Enable</i> , or <i>Forced</i> . The default is <i>Enable</i> .
Keep Alive Frequency	If NAT traversal is enabled or forced, type a keep-alive frequency setting (10-900 seconds). The default is 10. The value range is 10-900.
Dead Peer Detection	Select <i>Disable</i> , <i>On Idle</i> , or <i>On Demand</i> .

IPSec phase-2 fields

Create New IPSec Phase2

✕

* Tunnel Name:

The Tunnel Name field is required.

* Phase 1:

Test

▼

Advanced...

>

* Diffie-Hellman Groups:

☐ 1
 ☐ 2
 ☒ 5
 ☒ 14
 ☐ 15
 ☐ 16
 ☐ 17
 ☐ 18
 ☐ 19
 ☐ 20
 ☐ 21

* Key Life:

☒ Seconds
 ☐ KBytes
 ☐ Both

43200

(Seconds)

Auto Keep Alive:

☐

DHCP-IPsec:

☐

Quick Mode Selector

>

Save

Cancel

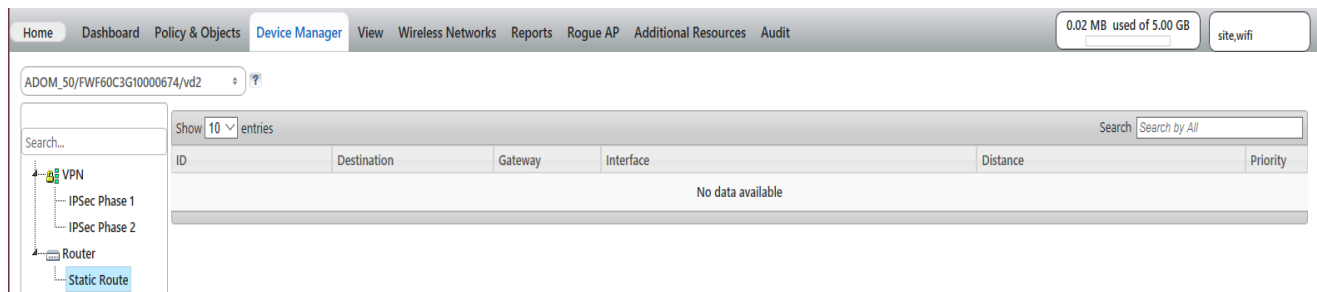
The Create New IPSec Phase2 and Edit IPSec Phase2 forms contain the following fields:

Settings	Guidelines
Tunnel Name	Required. Type a name for this Phase-2 configuration. The value is a string with a maximum of 35 characters.
Phase 1	Required. Select an IPSec Phase-1 configuration.
Advanced	
P2 Proposal	Select the encryption and authentication algorithms. You can select more than one. Use the arrows to move the algorithms from Available Encryption-Authentication Pair box to the Selected Encryption-Authentication Pair box.
Replay Detection	Select to enable or disable replay detection. Replay attacks occur when an unauthorized party intercepts a series of IPsec packets and replays them back into the tunnel. The default is selected.
Perfect forward secrecy (PFS)	Select to enable or disable perfect forward secrecy (PFS). Perfect forward secrecy (PFS) improves security by forcing a new Diffie-Hellman exchange whenever the key life expires. The default is selected.

Settings	Guidelines
Diffie-Hellman Groups	Required. Select one or more of the following Diffie-Hellman (DH) groups: 2, 5, 14, 15, 16, 17, 18, 19, 20, 21. At least one of the DH group settings on the remote peer or client must match one the selections on the FortiGate unit. Failure to match one or more DH groups will result in failed negotiations. Only one DH group is allowed for static and dynamic DNS gateways in aggressive mode. By default, 5 and 14 are selected.
Key Life	Required. Select the PFS key life. Select <i>Seconds</i> , <i>KBytes</i> , or <i>Both</i> . <ul style="list-style-type: none"> If <i>Seconds</i> is selected, type the number of seconds. The default is 43200. The value range is 120-172800. If <i>KBytes</i> is selected, type the number of KB. The default is 5120. The value range is 5120-4294967295. If <i>Both</i> is selected, type the number of seconds and the number of KB.
Auto Keep Alive	Optional. Select to enable or disable autokey keep alive. The phase 2 SA has a fixed duration. If there is traffic on the VPN as the SA nears expiry, a new SA is negotiated and the VPN switches to the new SA without interruption. If there is no traffic, the SA expires and the VPN tunnel goes down. A new SA will not be generated until there is traffic. The Autokey Keep Alive option ensures that a new SA is negotiated even if there is no traffic so that the VPN tunnel stays up. The default is deselected.
DHCP-IPsec	Optional. The default is deselected.
Quick Mode Selector	
Local Address	Select <i>Subnet</i> , <i>IP Range</i> , <i>IP Address</i> , or <i>Named Address</i> . <ul style="list-style-type: none"> If <i>Subnet</i> is selected, enter an IP address and netmask. If <i>IP Range</i> is selected, enter the first IP address and the last IP address in the range. If <i>IP Address</i> is selected, enter an IPv4 address. If <i>Named Address</i> is selected, select from the drop-down list.
Remote Address	Select <i>Subnet</i> , <i>IP Range</i> , <i>IP Address</i> , or <i>Named Address</i> . <ul style="list-style-type: none"> If <i>Subnet</i> is selected, enter an IP address and netmask. If <i>IP Range</i> is selected, enter the first IP address and the last IP address in the range. If <i>IP Address</i> is selected, enter an IPv4 address. If <i>Named Address</i> is selected, select from the drop-down list.
Local Port	Enter the number of the local port. The default is 0 The maximum value is 65535.
Remote Port	Enter the number of the remote port. The default is 0 The maximum value is 65535.
Protocol	Enter the protocol number. The default is 0 The maximum value is 255.

Routes ?

The Router tree under the Device Manager tab displays a list of static routes.



Configuring static routes

Use the Router area to define static routes.

In this area, the following actions are available:

- **Search**—enter text to search for in the table
- **Create New**—define a static route
- **Edit**—change an existing static route
- **Delete**—delete a static route

Adding a new static route

1. Select **Static Route** from the Router tree.
2. Right-click a static route and select **Create New Route**. If the table is blank, right-click under the column headings and select **Create New Route**.
3. Enter values in the relevant fields and select **Save**. See "**Static route fields**" on page 174.
4. Select **Save**.

Updating a static route

1. Select **Static Route** from the Router tree.
2. Right-click a static route and select **Edit**.
3. Update the values that have changed.
4. Select **Save**.

Deleting a static route

1. Select **Static Route** from the Router tree.
2. Right-click a static route and select **Delete**.

Static route fields

Create New Static Route

* Destination:

Subnet

0.0.0.0/0.0.0.0

* Interface:

ftp-proxy

* Gateway:

0.0.0.0

* Distance:

10

* Priority:

0

Comments:

0/255

Save

Cancel

The Create New Static Route and Edit Static Route forms contain the following fields:

Settings	Guidelines
Destination	Required. Select <i>Subnet</i> or <i>Named Address</i> for the destination. <ul style="list-style-type: none">If <i>Subnet</i> is selected, enter an IP address and netmask.If <i>Named Address</i> is selected, select from the drop-down list.
Interface	Required. Select the network interface that connects to the gateway from the drop-down list.
Gateway	Required. Enter an IPv4 address for the next hop.
Distance	Required. Enter the distance. The default is 10. The maximum is 255.
Priority	Required. Enter the priority. The default is 0. The maximum is 4294967295
Comments	Enter an optional description. The value is a string with a maximum of 255 characters.



FORTINET®

High Performance Network Security



Copyright© 2018 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.